Fertile grounds

van der Meulen, N.S.

Publication date:
2010

Document Version
Publisher's PDF, also known as Version of record

FERTILE GROUNDS:

The Facilitation of Financial Identity Theft in the United States and the Netherlands

FERTILE GROUNDS:
The Facilitation of Financial Identity Theft in the United States and the Netherlands

Proefschrift ter verkrijging van de graad van doctor
aan de Universiteit van Tilburg,
op gezag van de rector magnificus,
prof. dr. Ph. Eijlander,
in het openbaar te verdedigen ten overstaan van een
door het college voor promoties aangewezen commissie
in de aula van de Universiteit

op vrijdag 10 december 2010 om 14:15 uur

door

Nicole Samantha van der Meulen
Geboren te Naarden

Promotores:

Prof. dr. E.J. Koops
Prof. mr. J.E.J. Prins

Promotiecommissie:

Prof. mr. J.J.M. van Dijk
Prof. dr. M.J.G. van Eeten
Dr. C.J. Hoofnagle

This work is made possible through the subsidy programme of the Open Competition for the advancement of innovative and high-quality scientific research in the social sciences, which is financed by the Netherlands Organisation for Scientific Research (NWO).

Cover design:
U23 – Jordan Raeside

Production Wolf Legal Publishers
P. O. Box 31501, 6503 CB Nijmegen, The Netherlands
A commercial edition of this book will be published by TMC Asser Press.

In loving memory of Francy Elena Spence

CONTENTS

ABBREVIATIONS

BKR	Bureau Krediet Registratie
BSA	Bank Secrecy Act
BSN	Burgerservicenummer
CBP	College Bescherming Persoonsgegevens
CIA	Central Investigative Agency
CRA	Consumer Reporting Agency
CVC	Card Validation Code
DCC	Dutch Criminal Code
DPA	Data Protection Authority
DHS	Department of Homeland Security
DNB	De Nederlandsche Bank
DOJ	Department of Justice
DPPA	Drivers Privacy Protection Act
EDPS	European Data Protection Supervisor
EMV	Europay, MasterCard, VISA
EOUSA	Executive Office for United States Attorneys
EPIC	Electronic Privacy Information Center
EU	European Union
FACTA	Fair and Accurate Credit Transactions Act
FATF	Financial Action Task Force
FCRA	Fair Credit Reporting Act
FBI	Federal Bureau of Investigations
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FTC	Federal Trade Commission
GAO	Government Accountability Office
GBA	Gemeentelijke Basis Administratie
GLBA	Gramm-Leach Bliley Act
GOVCERT	Government Computer Emergency Response Team
GPEA	Government Paper Elimination Act
GSA	General Services Administration
HEC	Het Expertise Centrum
ICAO	International Civil Aviation Organization
ICE	Immigration and Customs Enforcement office
IDSP	Identity Theft Prevention and Identity Management Standards Panel
ITADA	Identity Theft Assumption and Deterrence Act
ITPEA	Identity Theft Penalty Enhancement Act
ITRC	Identity Theft Resource Center
KLPD	Korps Landelijke Politiediensten
MOB	Maatschappelijk Overleg Betalingsverkeer
NIST	National Institute of Standards and Technology
NVB	Nederlandse Vereniging van Banken
OCC	Officer of the Comptroller Currency
OMB	Office of Management and Budget
SAR	Suspicious Activity Report
SEPA	Single European Payments Area
SSN	Social Security Number

THTC	Team High Tech Crime
US-CERT	United States Computer Emergency Readiness Team
VIPS	Versterking Identiteitsketen Publieke Sector
WBP	Wet Bescherming Persoonsgegevens
WPR	Wet Persoonsregistratie

1 | Introduction

Tears begin to well up in the corner of his eyes as the camera captures his gaze. He holds up his hand before he faintly whispers 'a moment' as he collects himself to continue the story. Several seconds later, the National Ombudsman of the Netherlands appears before the camera. He describes the story of a single citizen who stands powerless against a State which appears ignorant of its own actions. For more than thirteen years, Ron Kowsoleea was known as a dangerous drug criminal. At first, he received a phone call from the Amsterdam police in 1994, asking him to come to the station. Once there, Kowsoleea discovered how a former schoolmate of his used his identity to escape prosecution for drug charges. The police officers register his story, but to no avail. Despite repeated attempts to clear his records, the problems continue. Several years later, on October 6, 2003, 35 armed police officers barge into his house and push him up against the wall in an effort to arrest him. Time and again Kowsoleea tries to demonstrate his innocence and explain the story of how someone else is using his identity; yet, all the charges and interaction with the police lead to the detriment of his name and reputation. The caption below the excerpt of the episode captures the essence of the story.[1] Identity theft, according to the caption, is no longer *just* an American problem. And there, at long last, was the victim to contradict those who considered identity theft a problem exclusively reserved for the United States.

1.1 Background

1.1.1 The Emergence of a Problem

Identity theft first appeared on the scene in the United States during the nineties. This is not to say identity theft did not exist prior to that. To the contrary, in the preface to his *Identity Theft Handbook*, Martin Biegelman reflects upon his experiences with 'identity theft' several decades ago.[2] Biegelman first became acquainted with identity theft in 1978, as a newly hired United States Postal Inspector. He describes how he heard fellow postal inspectors "…tell stories of fraudulent credit card applications and the resulting credit card frauds, the ease of obtaining personal information and phony identification to perpetrate this crime, how foreign nationals were behind many of the schemes, and how much money the banks and growing credit card industry were losing."[3] Based on these stories, Biegelman states how identity theft seemed like such a simple crime to commit. Several years after his initial encounter with the problem, Biegelman became part

---

[1] On October 23, 2008, *EenVandaag*, a daily current affairs show broadcast on public television, devoted part of its episode to the story of Ron Kowsoleaa, a victim of identity theft. Kowsoleea, who received media attention as a result of the response offered by the National Ombudsman, was falsely accused of 43 criminal offenses. The excerpt of the show is available online at http://www.eenvandaag.nl/buitenland/34037/tientallen_slachtoffers_identiteitsfraude (last accessed on July 4, 2010). For the full report of the National Ombudsman see http://www.nationaleombudsman.nl/rapporten/grote_onderzoeken/2007demonstreren/Dossier_hulp_voor_slachtoffer_fraude_metgestolenidentiteitskaart.asp (last accessed July 12, 2010).

[2] Biegelman, M. T. (2009). *Identity Theft Handbook: Detection, Prevention, and Security*. Hoboken, NJ: John Wiley & Sons, Inc.

[3] *Ibid:* xix.

of a team of federal agents assigned to investigate mail theft involving credit cards, checks, and other valuables sent via the post. Through his participation in the team of federal agents Biegelman received first hand experience with the perpetration of identity theft. A sense of urgency began to grow. Biegelman, together with his colleagues, tried to reach out in an effort to develop an awareness of the problem, since mere investigation and prosecution of perpetrators proved to be insufficient means to turn the tide. Despite several arrests, other perpetrators easily replaced those caught by the investigation team. Biegelman writes how it felt as though they were fighting a losing battle. On a video for employees of the TransUnion credit bureau, titled *Crime of the 80s*, Biegelman found another outlet for his outreach efforts. "I said things like 'It's a major problem throughout the country; the problem is growing so much that it is overwhelming law enforcement agencies; cooperation between banks, credit bureaus and law enforcement is essential to address the problem; and it's a growing problem and can destroy the credit industry as we know it if we don't stop it.'"[4]

The outreach continued during a United States Senate hearing in 1986 where Biegelman received the opportunity to testify and speak of the evolving threat of identity theft. Interestingly, the concept of identity theft is never mentioned by any of the witnesses; yet, as Biegelman notes, everyone was describing it during their testimony.

Several years after the United States Senate hearing, the problem of identity theft finally erupted. While those directly involved with the problem demonstrated an awareness of its existence, others failed to recognize the symptoms until the official diagnosis. Identity theft began to manifest itself in the media as an important topic worthy of daily attention, much the same as an epidemic. From a crime of the 80s, as noted above, identity theft had become the crime of the new millennium.[5] This label appears to be in large part the result of the intricate connection between its anticipated proliferation and the incorporation of advances made in the field of digital technology. Identity theft received and continues to carry the label of the nation's fastest growing crime.[6] Various newspapers began to describe how identity theft occurred[7] and how particular practices in society led to the enablement of the crime.[8] Perhaps the greatest impact came as a result of the stories of victims of identity theft. The media managed to eloquently capture the experiences of victims and transform them into stories which attracted the attention of readers.[9] These stories also invited the consideration of the public policy arena and served as an impetus to pass legislation (see section 3.1.1). Several years earlier, Biegelman already reflected on the experiences of victims during his testimony. In particular, he recognized, even then, how despite the acceptance of financial losses by the financial services sector, victims still experienced a negative

---

[4] *Ibid:* xix-xx.

[5] Hoar, S. B. (2001). Identity Theft: The Crime of the New Millennium. *Oregon Law Review*, Vol. 80: 1423 – 1447.

[6] Shadegg, J. B. (1999). Statement to the U.S. House Committee on Commerce & the House Subcommittees on Telecommunications, Trade and Consumer Protection, and on Finance. *Identity Theft: Is There Another You?* Joint Hearing, April 12, 1999 (Serial 106-16).

[7] Oldenburg, D. (1997). Identity Theft and Other Scams. *Washington Post*, November 3, 1997: D05.

[8] O'Harrow, R. (1998). Who's Got Your Number? Data Access Feeds a New Breed of Crime. *Washington Post*, March 10, 1998: A08.

[9] Hansell, S. (1996). Identity Crisis: When a Criminal's got Your Number. *New York Times*, June 16, 1996: 1.

impact as a result of the 'crime.' During his testimony, he specifically stated: "I know of cases where the people, a year or two after the fraud, and after they have contacted the credit bureaus to clear up their name, they still have problems getting credit, including credit cards, mortgages, and other loans."[10]

The enormous attention devoted to the topic of identity theft also came accompanied by many questions. As Biegelman noted above, hardly anyone used the concept of identity theft prior to the nineties. When identity theft, both as a concept and as a phenomenon became the center of attention, everyone demanded answers. What is identity theft? How big is the problem? Neither question proved easy to answer, for the 'novelty' of the crime meant answers were simply unavailable. The first question, what is identity theft, remains a topic of discussion (see chapter 2). This study uses the following definition: "'Identity 'theft' is fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool without that person's consent."[11]

The diverse types of identity theft also increase the complexity of the phenomenon. The most familiar type of identity theft is financial identity theft, which is the primary focus of this study.[12] Financial identity theft refers to the misuse of the identity of another person in an effort to unlawfully obtain financial benefits. Just as disagreements or variations exist about the definition of identity theft in general, they do about financial identity theft in particular as well. From a restricted perspective, financial identity theft refers exclusively to true name fraud.[13] This refers to an activity where perpetrators obtain sufficient personal information to open an account, request a credit card or apply for a mortgage in the name of the victim. A more comprehensive or broad approach to financial identity theft also includes account takeover, which refers to the misuse of existing account information in an effort to drain its assets. This study includes both types of financial identity theft, since with true name fraud as well as account takeover the identity of another person is the primary instrument used to obtain the financial assets.

Besides financial identity theft, other types of identity theft stand in its shadow. Even so, these types certainly deserve a brief moment of reflection. The second type is criminal identity theft. The story of the victim in the introduction provides an example of a case of criminal identity theft. With criminal identity theft the perpetrator commits a (serious) violation and provides a 'stolen' identity to escape the subsequent process or prosecution. When individuals become victims of criminal identity theft they may, for example, be initially stopped for a minor traffic violation, but upon checking their records the police officer finds a warrant out for their arrest for a serious crime like murder.[14] The lack of attention granted to criminal identity theft receives criticism from various sources.[15] Especially with

---

[10] Biegelman (2009): xx.

[11] Koops, E. J. & R. E. Leenes (2006). ID Theft, ID Fraud and/or ID-related Crime: Definitions matter. *Datenschutz und Datensicherheit*, Vol. 30 (9): 556.

[12] Newman and McNally (2005) have suggested that research should focus on each separate type of identity theft rather than attempt to understand, or empirically assess, identity theft as a solitary construct or singular phenomenon.

[13] This does not include the usage of a fictious 'identity' since this type of identity-related crime does not involve an individual victim whose identity has been 'stolen.'

[14] Binder, R. & M. Gill (2005). *Identity Theft and Fraud: Learning From the USA*. Perpetuity Research & Consultancy International Ltd.

[15] Perl, M. W. (2003). It's Not Always about the Money: Why the State Identity Theft Laws Fail to

respect to legislation proposed or passed which ignores the consequences of criminal identity theft for its victims.[16]

In addition to the problems associated with financial and criminal identity theft, the establishment of medical identity theft depicts yet another side to the problem. Medical identity theft occurs when the perpetrator uses the personal information, including the insurance details, of another person to obtain medical goods and services. The most dangerous consequence of medical identity theft is the inclusion of erroneous entries into existing medical records of the victims. The World Privacy Forum notes how despite the profound risk carried by medical identity theft, "...it is the least studied and most poorly documented of the cluster of identity theft crimes. It is also the most difficult to fix after the fact, because victims have limited rights and recourses. Medical identity theft typically leaves a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[17] The World Privacy Forum brought medical identity theft to the attention of the public through its research[18] and continues to emphasize its importance during the discussion of legislation proposed in the Congress.[19]

To develop a better understanding of how perpetrators carry out acts of identity theft, whether financial, criminal, or medical, Graeme R. Newman & Megan M. McNally identify three different stages.[20] The first stage is the acquisition of personal information. The second stage is the use of the previously acquired personal information in order to obtain, for example, financial assets in the name of the victim. The third, and final, stage of identity theft concerns the discovery of the crime by the victim[21]. The actual act of identity theft concerns the first two stages, for the third stage is purely focused on the aftermath once the crime has already occurred. To accomplish both stages, perpetrators of identity theft incorporate various modus operandi. For the first stage, the acquisition of personal information, an extensive repertoire of methods exists. The main distinction made throughout the literature is between methods which either include or exclude means of (digital) technology. The distinction is often referred

---

Adequately Address Criminal Record Identity Theft. *Journal of Criminal Law & Criminology*, Vol. 94: 169 – 208.

[16] Linnhoff, S. & J. Langenderfer (2004). Identity Theft Legislation: The Fair and Accurate Credit Transactions Act of 2003 and the Road Not Taken. *Journal of Consumer Affairs*, Vol. 38 (2): 204 – 216.

[17] World Privacy Forum (n.d.). The Medical Identity Theft Information Page. Available at: http://www.worldprivacyforum.org/medicalidentitytheft.html (last accessed July 4, 2010).

[18] Dixon, P. (2006). Medical Identity Theft: The Information Crime That Can Kill You. Available at: http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf (last accessed July 4, 2010).

[19] The World Privacy Forum emphasizes the applicability of the Red Flags rule for the Health Care sector. See Gellman, R. & P. Dixon (2009). *Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers*. Available at: http://www.worldprivacyforum.org/pdf/WPF_RedFlagReport_09242008fs.pdf (last accessed July 4, 2010).

[20] Newman, G. R. & M. M. McNally (2005). *Identity Theft Literature Review*. Research report submitted to the United States Department of Justice. Available at: http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf (last accessed July 4, 2010).

[21] There is another third stage which is rarely recognized or discussed. This is the stage where perpetrators of financial identity theft make the gains of the second stage liquid. Basically, perpetrators must turn credit cards or credit card numbers into actual financial gain, i.e. cash. This is generally a labor intensive process since credit cards can be used for purchases which must then in turn be sold again in an effort to actually make a financial as opposed to just a material profit. For more information see http://www.wired.com/techbiz/people/magazine/17-01/ff_max_butler (last accessed October 24, 2010).

to as high versus low tech methods. These methods are not necessarily mutually exclusive for hybrid forms certainly exist. Familiar methods used by perpetrators before the onset of the digital era include dumpster diving and stealing mail from mailboxes. Dumpster diving refers to the act of rummaging through the trash of others in an effort to potentially collect personal information. This could be done both for residential as well as business trash.

Throughout the years, other methods evolved. The incorporation of social engineering techniques proved a popular means for information acquisition. Since social engineering maintains different meanings in different fields, it is important to clarify that social engineering with respect to (computer) security refers to a practice whereby information is obtained under false pretenses. Phishing remains a prime example of social engineering in contemporary society. During a phishing attempt, perpetrators of identity theft send an email in the name of an organization, usually a financial service provider, and claim the recipient must follow a link or download an executable file in order to reconfirm the personal information maintained by the organization.

Besides social engineering techniques, perpetrators also incorporate the usage of malicious software which provides them with the ability to capture all keystrokes through the installation of, for example, keyloggers, which in turn give perpetrators the desired personal information. Such usage of malicious software allows perpetrators to capture the personal information stored and processed by government agencies, financial service providers, payment processors, information brokers, and consumers. This demonstrates the exponential growth of the amount of personal information perpetrators of financial identity theft could capture through the usage of digital technology.

The second stage, on the other hand, focuses on the misuse of the previously acquired personal information. Based on the information captured during the first stage, perpetrators of financial identity theft attempt to either acquire a new credit card, loan, or mortgage or drain an existing bank account or credit card.

Overall, the existence of different types of identity theft demonstrates its complex and multi-faceted nature. This also increases the challenge of the establishment of a definition of the problem. Even so, through the Identity Theft Assumption and Deterrence Act of 1998 (see section 3.1.1) the United States managed to fill the void and provide a definition of the phenomenon. The establishment of a legal, albeit criminal, definition of the problem provided an instrument to answer the subsequent question which proved to be on the minds of many. This question revolved around the size of the problem.

1.1.2 Prevalence

The first official indications of a problem came from TransUnion LLC which received 35,235 consumer complaints about identity theft in 1992.[22] Years later, the passage of the previously mentioned Identity Theft and Assumption Deterrence Act of 1998 also led to the establishment of a consumer complaint center. On November 1, 1999 the Identity Theft Data Clearinghouse began to receive consumer complaints via a toll-free telephone number, 1-877-ID THEFT

[22] Katel, P. (2005). Identity Theft: Can Congress Give Americans Better Protection? *The CQ Researcher*, Vol. 15 (22): 517 – 540.

(438-4338).[23] Since 2000, the Identity Theft Data Clearinghouse has published its statistics on the complaints received from consumers.[24] During its first publication, the Identity Theft Data Clearinghouse recorded a total of 31,140 victims. The following years this number of complaints began to grow (see Table 1.1).

Table 1.1
Identity theft consumer complaints received per year (United States[25])

Year	Complaints received
2000	31,140
2001	86,250
2002	161,977
2003	215,240
2004	246,909
2005	255,687
2006	246,214
2007	259,314
2008	314,484
2009	278,078

The steady escalation of the number of complaints seemed to confirm the earlier statements made by Biegelman about the existence of a growing problem. The Government Accountability Office (GAO)[26] noted in 2002 how the prevalence of identity theft appeared to be on the rise.[27] Yet, the most recent number of complaints recorded in 2009 and published in 2010 demonstrates the first decline in a decade. Whether this is merely a fluke as opposed to the start of a promising trend is difficult to assess at the moment. Despite the decline, identity theft remains the number one consumer complaint received by the Federal Trade Commission (FTC).[28]

Besides the consumer complaint data, various other studies attempted and continue to attempt to shed light on the prevalence of the problem. Several studies came out in 2003. The first was the Privacy & American Business Survey which

---

[23] Federal Trade Commission (2003). *REPORT: Federal Trade Commission Overview of the Identity Theft Program*. Available at:
http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/ftc_overview_id_theft.pdf (last accessed July 4, 2010).
[24] Federal Trade Commission (2001). *Identity Theft Victim Complaint Data*. Available at:
http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/clearinghouse_2000.pdf (last accessed July 4, 2010).
[25] Federal Trade Commission (2010). *Consumer Sentinel Network Data Handbook for January – December 2009*.
[26] Until 2004, the Government Accountability Office was known as the General Accounting Office. Throughout the main text in the book (excluding footnotes), I refer to the agency as the Government Accountability Office regardless of the year in which the report was published.
[27] General Accounting Office (2002). *Identity Theft: Prevalence and Cost appear to be Growing*. Report to Congressional Requesters, GAO-02-363.
[28] The Federal Trade Commission also receives other (fraud) complaints from consumers.

concluded how a total of 33.4 million[29] individuals in the United States had become a victim of identity theft since 1990, and over 13 million since January 2001.[30] The study build on previous surveys held to assess the size of the identity theft problem.[31] Nearly parallel to the publication of the Privacy & American Business Survey, Gartner, Inc. reported a total of seven million victims of identity theft, through a mail survey of 2,445 households.[32] For the FTC, Synovate conducted more than 4,000 telephone interviews in an effort to develop an estimation of the number of identity theft victims. Based on the interviews, Synovate concluded how 27.3 million Americans had become a victim of identity theft during the previous five years.[33] Of that number, nearly ten million became a victim during the previous year alone.[34]

The studies continued during the following years. Javelin Strategy & Research became engaged in the debate and reported in 2005, in conjunction with the Better Business Bureau, how identity theft had established 9.3 million victims during the previous year.[35] This was a decrease in comparison to the results published by Synovate in 2003 and as such led certain sources to conclude how "…fears of identity theft being a rapidly growing problem are exaggerated."[36] This became the start of a zesty debate over the reliability of the results provided. The original decrease published in 2005 continued the following year, when Javelin reported how 8.9 million individuals had become a victim of identity theft during the previous year.[37] This trend returned in 2007 when Javelin updated its study and concluded how the total number of victims had once again declined to 8.4 million.[38] This in contrast to other results published around the same time. Gartner, Inc. returned in 2007 with a prevalence study on identity theft and concluded a fifty percent increase over its 2003 results. The total number of identity theft victims grew from seven to fifteen million.[39] Simultaneously, the FTC published its yearly consumer complaint data which indicated how identity theft remained the leader in terms of consumer complaints received by the clearinghouse. The proximity of publication accompanied by the diverse and conflicting nature of the results led many to question the reliability and the validity of the data. Especially the reports published by Javelin became the object of increased scrutiny since Javelin Strategy & Research receives financial support from organizations active in the financial services industry.[40] Whereas Javelin

---

[29] This estimation is based on a representative sample of respondents of which 16% reported being a victim of identity theft in the past.

[30] Harris Interactive (2003). *Identity Theft New Survey & Trend Report*. Commissioned by Privacy & American Business.

[31] The 1998 and 1999 surveys asked respondents the following question:
"Have you or any member of your family ever been the victim of identity fraud? This is where someone uses a lost or stolen credit card or false identification to obtain merchandise, open credit or bank accounts or apply for government benefits in someone else's name?" In 1998, 20% provided an affirmative answer and the following year the percentage (21) was nearly identical.

[32] Gartner (2003). Gartner Says Identity Theft is up Nearly Eighty Percent. *Press Release*, July 21, 2003.

[33] Synovate (2003). *Federal Trade Commission – Identity Theft Survey Report*.

[34] *Ibid*.

[35] Javelin Strategy & Research (2005a). *2005 Identity Fraud Survey Report*. Consumer Version.

[36] Lenard, T. M. & P. H. Rubin (2006). Much Ado About Notification. *Regulation*, Vol. 29 (1): 44.

[37] Javelin Strategy & Research (2006). *2006 Identity Fraud Survey Report*. Consumer Version.

[38] Javelin Strategy & Research (2007a). *2007 Identity Fraud Survey Report*. Consumer Version.

[39] Gartner (2007). Gartner Says Number of Identity Theft Victims Has Increased More Than 50 Percent Since 2003. *Press Release*, March 6, 2007.

[40] CheckFree, an electronic payment company, is a sponsor of Javelin's research and in its reports

prides itself as an independent organization, such financial support leads to an inevitable suspicion for the industry maintains a vital interest in the publication of prevalence data. As Chris Jay Hoofnagle notes, "[i]dentity theft is a high-stakes issue in the public policy world. It is a popular issue for political candidates, who have proposed many laws with serious implications for lending institutions. Because identity theft brings regulatory attention to lending institutions, there is a great pressure to redirect the attention elsewhere."[41] As a result, Hoofnagle argues how the press releases published by research corporations like Javelin are a tactic to provide an indication for a decline in identity theft cases. This published decline subsequently helps the survey's sponsors to redirect the attention of policy makers. The projected decline of identity theft cases by Javelin came to an end in 2008 when identity theft began to rise and the total number of victims estimated was nearly ten million.[42] When Javelin published its most recent conclusions in 2010, the number of identity theft victims reached an all time high. More than 11 million individuals became victims of identity theft in 2009, according to Javelin's research.[43]

The increase of identity theft cases published over the previous two years appears to mitigate the arguments against Javelin, but there are other aspects discussed in the conclusions provided by the research organization which do support Hoofnagle's notion of attention diversion. Javelin writes how "[m]any identity thefts can occur through traditional methods such as stolen wallets and 'friendly frauds,' in which the crime is committed by a person known to the victim. In fact, among the victims who knew how their data was taken, lost or stolen wallets, checkbooks, or credit cards accounted for nearly two times as many instances of theft as all online attack methods combined. Identity theft occurrences are often the result of the most remedial and simple ways to steal information, not through hacking or elaborate Internet schemes."[44] This is not the first time Javelin came to this conclusion. The 'controversial' study published in 2007 made similar claims, which Hoofnagle recognizes and rightfully challenges.[45] The problem with the statements made by Javelin about the origin of the personal information misused for identity theft purposes is its reliance on victims who actually think they know how perpetrators obtained the information. This group is a minority of those used for the data collection which Javelin bases its conclusions on. Even so, Javelin uses this information to draw broad conclusions and neglects the remainder and majority of victims who are unaware of the method of information collection used by the perpetrators. The diversion of attention accomplished through these statements is successful, since Javelin aims to demonstrate how predominantly consumers maintain the ability to control incidents of financial identity theft. Others accept this information as a 'fact' and use the conclusions to support their own arguments.[46]

Javelin recommends consumers to transfer to electronic banking, as a means to reduce the risk of financial identity theft. This recommendation, however, does not appear to be based on the actual data collected and analyzed by Javelin.

[41] Hoofnagle, C. J. (2007). Identity Theft: Making the Known Unknowns Known. *Harvard Journal of Law and Technology*, Vol. 21 (1): 119.

[42] Javelin Strategy & Research (2009). *2009 Identity Fraud Survey Report*. Consumer Version.

[43] Javelin Strategy & Research (2010). *2010 Identity Fraud Survey Report*. Consumer Version.

[44] *Ibid:* 7.

[45] Hoofnagle (2007): 100.

[46] Fred H. Cate (2004), for example, stated during his testimony for the U.S. House Subcommittee on Social Security of the Committee on Ways and Means how "[w]hile we do not know as much as we

This discussion leads into a more vital aspect of prevalence studies. This is the investigation of how perpetrators manage to complete the act of financial identity theft. The importance of this research is the development of an understanding of how the crime occurs and as a result to reveal the vulnerabilities present in contemporary society. Even so, the near obsession with the accumulation of prevalence data on identity theft often overshadows the importance of this type of research. Moreover, an actual determination of how financial identity theft occurs, especially how perpetrators acquire the personal information needed to move on to the second stage of the crime, is particularly difficult to determine (see section 1.4).

1.1.3 Victims

Besides the attention devoted to the statistical prevalence of the problem, interest groups began to investigate the experiences of the victims of the crime. The horror stories of victims described by the media demonstrated the consequences of the problem. These stories led identity theft to receive the label of a crime which is "...insidious, complex and potentially devastating."[47] The media attention devoted to the stories of victims of identity theft proved to be in stark contrast to the neglect demonstrated by the law enforcement community. For victims of identity theft encountered significant challenges during the early years to receive recognition as victims of a crime. This was mainly due to the 'novelty' of identity theft and its absence in the code of criminal law. The United States changed this discrepancy in 1998 through the Identity Theft Assumption and Deterrence Act.

The Australasian Centre for Policing Research (ACPR) recognizes three different types of impact: direct and indirect financial impacts and the psychological impact of the crime.[48] The experiences of victims with regard to these different types of impact return in various studies.[49] The Privacy Rights Clearinghouse paved the way through an overview study of victims and their experiences in 2000.[50] The organization spoke to 66 victims of identity theft and produced a groundbreaking document, *Nowhere to Turn*. In its findings, the Privacy Rights Clearinghouse describes how victims of identity theft spent an average of 175 hours actively trying to resolve their case. Victims generally need to contact the creditor, the debt collector, and the consumer reporting agencies (CRAs) in an attempt to remove the bad credit charges from their records. The inaccurate bad credit charges ignite the most problems because they generally prevent victims from obtaining a new credit card, opening a bank account, renting an apartment, or even finding a job. These findings are not extraordinary as later studies prove. Since 2003, the Identity Theft Resource Center (ITRC) produces a comprehensive

---

need to know about identity theft, thanks to the efforts of FTC and others, one important fact we are learning is that much—perhaps most—identity theft is not committed by a stranger but by a family member, friend, or co-worker."

[47] Crenshaw, A. B. (1996). Identity Crisis: the theft that's tough to thwart. *Washington Post*, 25 August 1996: H01.

[48] Australasian Centre for Policing Research (ACPR) (2006). *Review of the legal status and rights of victims of identity theft in Australasia.*

[49] Important to note is the selection bias present in the studies since the victims who contact the respective organizations tend to be worse off than most.

[50] Privacy Rights Clearinghouse (2000). *Nowhere to Turn: Victims Speak Out on Identity Theft* - A Survey of Identity Theft Victims and Recommendations for Reform. Available at: http://www.privacyrights.org/ar/idtheft2000.htm (last accessed July 5, 2010).

and thorough analysis on a periodic basis about the long-term impact of identity theft on its victims. Through in-depth surveys, the ITRC attempts to surpass previous studies conducted by the FTC, the GAO, and consumer groups to explore other areas of victimization.[51]

According to the 2003 analysis provided by the ITRC, victims of identity theft spent an average of 600 hours to resolve or at least try to resolve their case – considerably longer than the 175 hours reported by the Privacy Rights Clearinghouse.[52] This number began to fluctuate and decrease throughout the following years, from 330 hours in 2004[53] to 141 hours in 2009.[54] The decrease in hours spent by victims in an effort to repair the damage caused by perpetrators of identity theft proved to be a source of positive support for the ITRC, which actually commenced its report in 2010 by stating how "[f]or the first time in seven years, the Identity Theft Resource Center (ITRC) can state that it is encouraged by the findings of the *Identity Theft: The Aftermath 2009*."[55]

Besides hours spent on damage recovery, studies also demonstrate an interest in the emotional or psychological impact of the crime on its victims. Tracy Sharp *et al.* conducted an exploratory study to assess the psychological and somatic impact of identity theft, as well as the coping mechanisms used by victims.[56] For their study, Sharp *et al.* recruited 37 identity theft victims and placed them in six focus groups. The researchers provided the victims with two victim impact questionnaires. The first was administered two weeks after the victims discovered the incident of identity theft and the second six months after the discovery. The results of the first questionnaire indicated the following common reactions: irritability and anger, fear and anxiety, and frustration. During the second impact measurement, the results demonstrated how "…the emotional responses shifted such that the majority (26%) of participants indicated that they were distressed and desperate, 24% stated that they were irritated and angry, and 14%...endorsed feelings of anxiety, fear, mistrust and paranoia."[57] Victims of identity theft thus experience similar feelings as victims of other crimes. Consequently, they generally need and deserve treatment which other victims have a right to during the aftermath of a crime. Sharp *et al.* recognize how "[t]he results of this study suggest that psychological impact is indeed great on victims of identity theft. Not only are there immediate emotional and physical consequences to the victimization, but also lasting effects are seen, especially in cases that have not met resolution."[58] The ITRC demonstrates similar results since the organization found many victims who in the short term felt defiled (37%) and betrayed (60%).[59] Victims also acknowledged feelings of a loss of innocence (21%), and a sense of powerlessness (63%). Long-term feelings experienced by victims included the inability to trust people (30%), suicidal thoughts (4%), being ready to give up the fight (25%), and the belief to have lost everything (10%).[60] The ITRC results of 2009 did, however,

---

[51] Identity Theft Resource Center (2004). *Identity Theft: The Aftermath 2003*.
[52] *Ibid.*
[53] Identity Theft Resource Center (2005). *Identity Theft: The Aftermath 2004*.
[54] Identity Theft Resource Center (2010a). *Identity Theft: The Aftermath 2009*.
[55] *Ibid:* 2.
[56] Sharp, T., Sherver-Neiger, A., Fremouw, W., Kane, J. & S. Hutton (2004). Exploring the Psychological and Somatic Impact of Identity Theft. *Journal of Forensic Science*, Vol. 49 (1): 131 – 136.
[57] *Ibid:* 132
[58] *Ibid:* 133 – 134.
[59] Identity Theft Resource Center (2009). *Identity Theft: The Aftermath 2008*.
[60] *Ibid.*

indicate a decrease in internal negative attitudes held by victims, such as guilt, shame, being undeserving of help, or feeling captive or suicidal.

Whereas victims of identity theft demonstrate similar emotional expressions as victims of other crimes, they are simultaneously subject to a particular breed of secondary victimization. This is an aspect which is inherent to fraud victims and the way society perceives them. Henry Pontell *et al.* describe how "…elements inherent in fraud victimization may reinforce public and victim perceptions that they acted foolishly, and are therefore more blameworthy with regard to their own victimization."[61] This can in turn increase the psychological impact of the crime.

1.1.4 Beyond the United States

As the United States expanded its experience with identity theft and increased its knowledge about the crime, other countries also began to open their eyes as the threat of identity theft began to spread much like the contamination of an infectious disease.[62] Whereas originally other countries delighted in a sense of immunity, identity theft proved to be something other than an expression of American exceptionalism. The United Kingdom[63] began to devote attention to the topic, just as Canada[64] and Australia.[65] Besides the Anglo-Saxon countries, others such as the Netherlands also referred to and identified identity theft as a problem of public policy.[66] On a transnational level, the European Union,[67] the United Nations,[68] the Council of Europe,[69] and the Organisation for Economic Cooperation and Development (OECD)[70] all became involved.

The questions which dominated the debate in the United States also returned in other countries and transnational organizations. The discussion about the definition proved to be a source of major attraction as did the quest for empirical data to assess the size of the problem.[71] For the United Kingdom, the Credit Industry Fraud Avoidance System (CIFAS) has collected consumer complaints since 1999 (see Table 1.2).[72]

---

[61] Pontell, H. N., Brown, G. C. & A. Tosouni (2008). "Stolen Identities: A Victim Survey," in Megan M. McNally and Graeme R. Newman (eds.), *Perspectives on Identity Theft. Crime Prevention Studies*, Vol. 23. Monsey, NY: Criminal Justice Press: 58.

[62] See van der Meulen, N. S. (2007). The Spread of Identity Theft: Developments and Initiatives within the European Union. *The Police Chief*, Vol. 74 (5): 59 – 61.

[63] United Kingdom Cabinet Office (2002). *Identity Fraud: A Study*. United Kingdom: Cabinet Office Publications.

[64] See for example Cavoukian, A. (1997). *Identity Theft: Who's Using Your Name?* Information and Privacy Commissioner/Ontario.

[65] Cuganesan, S. & D. Lacey (2003). *Identity fraud in Australia: an evaluation of its nature, cost and extent.* Standards Australia International.

[66] *Kamerstukken II* 2001 – 2002, 17050, nr. 234.

[67] Europol (2003). *2003 European Union Organised Crime Report*; Mitchison, N., Wilikens, M., Breitenbach, L., Urry, R. & S. Portesi (2004). *Identity Theft: A Discussion Paper*. European Commission Joint Research Center.

[68] The United Nations Crime Commission has established an Intergovernmental Expert Group on Fraud and the Criminal Misuse and Falsification of Identity.

[69] Gercke, M. (2007). *Project on Cybercrime: Internet-related identity theft*. Discussion paper Economic Crime Division Directorate General of Human Rights and Legal Affairs.

[70] Organisation of Economic Co-Operation and Development (OECD) (2009). *Online Identity Theft*, OECD Publishing. See also OECD (n.d.). *Report on Identity Fraud: Tax Evasion and Money Laundering Vulnerabilities*. Centre for Tax Policy and Administration.

[71] Van der Meulen, N. S. & E. J. Koops, eds. (2008). *D 12.7: Identity-related crime in Europe – Big Problem or Big Hype?* Available at: http://www.fidis.net.

[72] Credit Industry Fraud Avoidance System (CIFAS) (2010). Is ID fraud serious? Available at:

Table 1.2
Identity theft consumer complaints received per year (United Kingdom[73])

Year	Cases recorded
1999	9,000
2000	16,000
2001	24,000
2002	34,000
2003	46,000
2004	56,000
2005	66,000
2006	80,000
2007	77,500
2008	77,600

The number of cases recorded by CIFAS demonstrates a steady increase until 2006. The following years, 2007 and 2008, instead demonstrate a state of relative stability. Other sources of data which provide an indication of the problem come from cost estimates provided by the Cabinet Office. The Cabinet Office of the United Kingdom published a report in February 2006 which determined how their economy suffered a financial loss of £1.7 billion per year as a result of identity fraud.[74] Several years prior, in 2002, the Cabinet Office estimated a loss of £1.3 billion per year. The Cabinet Office emphasizes the limited nature of the statistical data since the data relies exclusively on available figures which fail to provide an accurate reflection of the entire figure.[75]

The Home Office also published statistics on plastic card and identity fraud in 2007. These statistics are the findings of the 2005/06 British Crime Survey.[76] Of all the respondents using plastic cards, four per cent became a victim of fraud during the previous year. The survey also provides data on identity fraud through the misuse of personal information. According to the findings, two per cent of respondents became a victim to this type of identity fraud.[77]

Other countries maintain limited indications of the size of the problem. For Canada, PhoneBusters, an organization which analyzes and reports on incidents of identity theft, reportedly received 13,359 consumer complaints in 2003 as compared to 8,187 in 2002.[78] During later years, the number of identity theft

---

http://www.cifas.org.uk/default.asp?edit_id=968-56 (last accessed July 5, 2010).

[73] It is unclear whether these numbers contain both true name fraud and account take over cases.

[74] United Kingdom Home Office (2006). Updated Estimate of the Cost of Identity Fraud to the UK Economy. Available at:
http://www.identitytheft.org.uk/cms/assets/cost_of_identity_fraud_to_the_uk_economy_2006-07.pdf (last accessed July 5, 2010).

[75] United Kingdom Cabinet Office (2002).

[76] Home Office Statistical Bulletin (2007). *Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey.* Available at:
http://www.homeoffice.gov.uk/rds/pdfs07/hosb1007.pdf (last accessed July 12, 2010).

[77] *Ibid.*

[78] Perrin, S. (2006). *PIPEDA and Identity Theft: Solutions for Protecting Canadians.* BC Freedom of Information and Privacy Association.

complaints demonstrates a marginal fluctuation from 10,637 complaints in 2007 to 12,232 in 2008, and back down to 11,979 in 2009.[79]

In the Netherlands, the lack of registration of identity theft as an individual crime complicates the collection of prevalence data. Despite the absence of statistical data on the prevalence of the problem, various sources identified identity theft as a rising phenomenon[80] or a growing concern.[81] This primarily concerned the potential proliferation of financial identity theft in the Netherlands; yet, its criminal counterpart demanded the most attention after Jan Grijpink stated how more than 101.000 identity fraudsters could be located in the automated fingerprint system *Havank* of the Dutch police.[82] Through the provision of this empirical data, all eyes turned to the criminal justice system. For the thought of criminals on the loose in the Netherlands invited the interest of the media.[83] The Lower House in turn also found itself compelled to respond and demand action. The Ministry of Justice responded to the increased attention by describing its awareness of the problem and its ongoing efforts to reduce it.[84]

For financial identity theft, the Dutch tide with respect to prevalence data began to turn a couple of years later when at the start of 2010, the National Complaint Center, which commenced its operation at the end of 2008, published its final report on the pilot study conducted during the previous year.[85] This study provides perhaps the first official indication of the size of the problem. During the year 2009, the complaint center received 349 consumer 'complaints.'[86] This total number includes consumers who merely contacted the center for information. The actual number of complaints which concerned identity theft or at least the suspicion of its existence was 241. The generalizability of this number is difficult to establish, since the complaint center aimed to maintain a low profile throughout its pilot year. This mainly as a result of the lack of financial resources invested in the project which led to a limited staff and as such limited capabilities. The potential impact of the low profile maintained by the complaint center became evident when the center received media attention in October 2009.[87] In October, the number of complaints received by the center reached its peak which appears to be directly related to the attention granted to the center by the media and the rise in awareness among the public about its existence.

Prior to the existence of a public consumer complaint center, a private initiative aimed to get a grip on the prevalence situation. Fellowes, a company which grants substantial attention to the problem of identity theft as a result of its marketing of paper shredders, conducted a study and published data on the

---

[79] Canadian Anti-Fraud Centre Criminal Intelligence Analytical Unit (2010). *Mass Marketing Fraud & ID Theft Activities.* Annual Statistical Report 2009.

[80] Rabobank Groep (2009). *Maatschappelijk jaarverslag 2008: Verantwoord bankieren voor een duurzame toekomst*: 32.

[81] Maatschappelijk Overleg Betalingsverkeer (MOB) (2006). *Rapportage Maatschappelijk Overleg Betalingsverkeer 2005*; *Kamerstukken II* 2003 – 2004, 29 200 VI, nr. 166; Openbaar Ministerie (OM) (2006). *Perspectief op 2010*.

[82] Grijpink, J. H. A. M. (2006). Identiteitsfraude en overheid. *Justitiële Verkenningen*, Vol. 32 (7): 37 – 57.

[83] See for example de Witt, R. (2006). Veel criminelen laten anderen straf uitzitten. *Elsevier.* Available at: http://www.elsevier.nl/web/Nieuws/Nederland/98552/Veel-criminelen-laten-anderen-straf-uitzitten.htm (last accessed July 12, 2010).

[84] Directoraat-Generaal Rechtspleging en Rechtshandhaving (2006). Identiteitsvaststelling in de strafrechtketen.

[85] Centraal Meldpunt Identiteitsfraude (2010). *Jaarrapportage 2009*.

[86] *Ibid.*

[87] *Ibid.*

prevalence of identity theft.[88] Fellowes surveyed 500 citizens in 2009 and 1000 citizens in 2008. Based on the responses to the surveys, Fellowes estimated how 130.000 citizens have been a victim of identity theft in the Netherlands.[89] Whether this number refers to the total number of identity theft victims ever or to a particular time period remains unclear. Due to the commercial interest of Fellowes, its publication of data on the prevalence of identity theft is difficult to gage in terms of reliability and validity. Much the same as the problems associated with the publication of the results provided by Javelin Strategy & Research in the United States.

As a result, public prevalence data on financial identity theft in the Netherlands remains scarce; yet, there is an overall air of potential urgency about identity theft.[90] The focus therefore should be on an analysis of the presence of vulnerabilities in the Netherlands which can facilitate the occurrence of financial identity theft. Such an analysis can in turn provide a necessary reflection on the potential for the development of a problem despite the absence of prevalence data on the phenomenon. The lack of such an analysis shall otherwise allow opponents to render claims about the potential for identity theft as a rising phenomenon or a growing concern as merely speculative and as such without value.

1.2 Theoretical Framework and Research Question

The original focus of criminological theory in an effort to develop an understanding of the causes of crime was on offenders. The primary spotlight was on the *why* as opposed to the *how*. This changed during the 1970s and 1980s when a variety of different but complementary perspectives emerged which shifted the focus away from offenders and onto society. These perspectives came largely in response to the vain impact of conventional criminology in the area of crime prevention and crime control. As Ronald V. Clarke notes, "…the dispositional bias remains and renders criminological theory unproductive in terms of the preventive measures it generates."[91] David Garland refers to this new genre as "the new criminologies of everyday life" and recognizes how this "new style of criminological thinking" proved particularly successful in attracting the attention of government officials.[92] The new criminologies of everyday life refer to a collection of related theoretical perspectives. The main premise shared by all perspectives is the view of crime as a normal and commonplace aspect of contemporary society. This in contrast to earlier theoretical perspectives used in criminology, which maintained the premise of crime as a deviation from normal civilized conduct and explained its occurrence via individual pathology or faulty

---

[88] Fellowes (2009). Nederlander niet bewust van risico identiteitsfraude. *Press Release.* Available at: http://www.fraudevoorkomjezelf.nl/downloads/Nederlander_niet_bewust_van_risico_identiteitsfraude.pdf (last accessed July 8, 2010).

[89] *Ibid.*

[90] See Prins, J. E. J. (2003). Het BurgerServiceNummer en de strijd tegen de Identiteitsfraude. *Computerrecht*, (1): 2-3; Prins, J. E. J. (2006). Variaties op een thema: van paspoort- naar identiteitsfraude. *Nederlands Juristenblad*, Vol. 81: 9-14.

[91] Clarke, R. V. G. (1980). 'Situational' Crime Prevention: Theory and Practice. *British Journal of Criminology*, Vol. 20 (2): 137.

[92] Garland, D. (2001). *The Culture of Control: Crime and Social Order in Contemporary Society*. Oxford: Oxford University Press: 127.

socialization.[93] Since the emergent perspectives departed from a different premise, the explanations developed for the causes of crime also differed. The explanations offered focus on the situational context of crime which provides information on measures to take in an effort to reduce the likelihood of specific crimes to occur.

Various complementary perspectives play a role in 'unconventional' criminology. As Clarke recapitulates, "[e]nvironmental criminology, the rational choice perspective, and routine activity and lifestyle theories have all helped to strengthen situational prevention in different ways, reflecting their different origins and the purposes for which they were developed."[94] All together these theoretical perspectives provide assistance for the development of an opportunity structure for crime. The routine activity approach, developed by Lawrence E. Cohen and Marcus Felson, specifically concentrates on the circumstances in which perpetrators of crime carry out their activities. The main argument set forth by Cohen and Felson is how structural changes in routine activity patterns have the potential to influence crime rates. This influence occurs through the impact of such changes on the 'convergence' in space and time of three elements of direct-contact predatory violations. These elements include motivated offenders, suitable targets, and the absence of capable guardians against a violation. The suitability of targets is based upon four components derived from a human ecological background. These four components are value, visibility, access, and inertia.[95] The concept of a target refers both to potential victims and to material objects. Cohen and Felson write how "…the probability that a violation will occur at any specific time and place might be taken as a function of the convergence of likely offenders and suitable targets in the absence of capable guardians."[96] The absence of any single element leads to possible prevention of the violation. This demonstrates the interdependency, as Cohen and Felson note, between illegal acts and routine activities in everyday life. Such interdependency leads Cohen and Felson to apply concepts from human ecological literature to the analysis of crime and crime rates. The ecological nature of illegal acts requires them to feed upon other activities. Cohen and Felson state how "[s]ince illegal activities must feed upon other activities, the spatial and temporal structure of routine legal activities should play an important role in determining the location, type and quantity of illegal acts occurring in a given community or society."[97] Whereas Cohen and Felson acknowledge how their ideas presented in their work are not new, theoretical literature in criminology has often overlooked such ideas. As such Cohen and Felson develop a framework of previously unconnected analyses of criminological aspects in society.

The framework set forth by Cohen and Felson establishes a connection between illegal and legal activities through a consideration of how everyday life brings together the three elements identified above in space and time. Felson added a fourth element to the equation which he terms the absence of 'the

---

[93] *Ibid:* 128.
[94] Clarke, R. V. (1995). 'Situational Crime Prevention,' in M. Tonry & D. P. Farrington (eds.) *Building a Safer Society: Strategic Approaches to Crime Prevention.* Chicago: University of Chicago Press: 101.
[95] Felson, M. & L. E. Cohen (1980). Human Ecology and Crime: A Routine Activity Approach. *Human Ecology*, Vol. 8 (4): 393.
[96] Cohen, L. E. & M. Felson (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review*, Vol. 44: 590.
[97] *Ibid.*

intimate handler.'[98] The intimate handler is someone 'close' to the offender and who is in a position to exert informal social control in an effort to prevent the crime. The idea of the intimate handler as an additional element is derived from the fundamentals of the social control theory as described by Travis Hirschi.[99] The four fundamentals of Hirschi's control theory are commitments, attachments, involvements, and beliefs. Felson subsequently combines these four elements and captures them through a single concept: handle. This handle is a necessary condition, according to Felson, for the occurrence of informal social control.[100]

Clarke in turn developed an argument to add a fifth element to the routine activity theory in an effort to enhance its contribution. This fifth element is crime facilitators, which includes diverse tools or features of everyday life which enable crime.[101] Examples provided by Clarke include automobiles, credit cards, and weapons, which, according to the author, are essential tools for various specific forms of crime.[102]

Many years after its introduction, the routine activity theory continues to demonstrate the applicability of the approach in contemporary society. Cohen and Felson foreshadowed such applicability through writing how "…one can analyze how the structure of community organization as well as the level of technology in a society provide the circumstances under which crime can thrive."[103] The reference to technology, in particular its usage and organization, is especially relevant to the topic of financial identity theft.[104]

Parallel to the introduction of the routine activity theory, Clarke introduced the 'situational' crime prevention theory.[105] Clarke described how practical options for prevention managed to arise from a greater emphasis placed on the situational features of crimes. Such an emphasis occurred during previous 'situational' research, which Clarke categorizes into two categories based on the measures introduced in light of prevention. The first category focuses on the reduction of physical opportunities for offenders and the second category places an emphasis on the increased risk for offenders to be caught for their crimes. Despite the distinction made by Clarke, he recognizes how certain preventative measures demonstrate attributes which allow them to fit into both categories.[106] Unlike previous theoretical perspectives in criminology, the situational crime prevention framework tailors its analysis and measures toward specific forms of crime, rather than criminality in general. This framework includes a standard action research methodology which consists of five sequential stages. These stages include the collection of data about the nature and dimensions of a specific crime problem, an analysis of the situational conditions which facilitate the commission of the crimes in question, and a systematic study of potential means to block opportunities for

---

[98] Felson, M. (1986). 'Linking Criminal Choices, Routine Activities, Informal Control, and Criminal Outcomes,' in D. B. Cornish & R. V. Clarke (eds.) *The Reasoning Criminal: Rational Choice Perspectives on Offending*. New York: Springer-Verlag: 119 – 128.
[99] Hirschi, T. (1969). *Causes of Delinquency*. Berkeley: University of California Press.
[100] Felson (1986): 121.
[101] Felson, M. (2006). *Crime and Nature*. SAGE Publishing: 71.
[102] Clarke (1995): 101.
[103] Felson & Cohen (1980): 393.
[104] This connection is eloquently demonstrated by Daniel J. Solove through his description of the architecture of vulnerability. See Solove, D. J. (2003) Identity Theft and the Architecture of Vulnerability. *Hastings Law Journal*, Vol. 54: 1227 – 1276.
[105] Clarke (1980).
[106] *Ibid.*

the specific crime problems. The last two stages focus on the implementation of the most promising countermeasures and the monitoring of results.[107]

Throughout the years, Clarke considerably expanded the situational crime prevention approach. He added another category of measures introduced to prevent the occurrence of specific crimes. This category focuses on reducing the rewards. Based on these three categories, Clarke identified a total of twelve techniques which together compose a framework for situational crime prevention.[108] Under the umbrella of increasing the effort, Clarke identified the following options: target hardening, access control, deflecting offenders, and controlling facilitators.[109] For increasing the risks, Clarke introduced the following four groups of measures: entry/exit screening, formal surveillance, surveillance by employees, and natural surveillance. And the last category of reducing rewards includes target removal, identifying property, removing inducements, and rule setting. The expansion continued when Clarke added another category to his existing framework in 1997.[110] This fourth category identifies the potential for removing excuses as a means to reduce opportunities. Removing excuses can be accomplished through four separate techniques, including rule setting, stimulating conscience, controlling disinhibitors, and facilitating compliance.[111] This situational prevention framework is an important source of guidance for the analysis of existing and potential countermeasures, but also works in the opposite direction to observe how the absence of such techniques develop and enhance the existence of an opportunity structure for specific crimes.

Earlier applications of the complementary theoretical perspectives to terrorism[112] and e-commerce crimes[113] demonstrate the relevance of this theoretical framework to financial identity theft. Moreover, Graeme R. Newman writes how, "[a]ny attempt to reduce the extent of identity theft must be aimed at the source of the problem, which lies not with the motivation of likely offenders but with the technological, business, and economic arrangements that create opportunities for identity thieves to carry out crimes and at the same time provide the factual basis for their rationalizations."[114] As a result, the development of an opportunity structure, or rather a facilitation framework, of identity theft has been selected as the point of departure of the current research project. Based on the framework developed by the above discussed theories, this study aims to answer the following central research question:

How do states, financial service providers, consumers, and others facilitate the occurrence of financial identity theft in the United States and the Netherlands? And what are the implications for existing countermeasures and how do these fit into the situational crime prevention framework?

---

[107] Clarke (1995).
[108] Clarke, R. V. (1992). 'Introduction,' in R. V. Clarke (ed.) *Situational Crime Prevention: Successful Case Studies*. Albany, NY: Harrow and Heston Publishers: 3 – 36.
[109] *Ibid:* 13.
[110] Clarke, R. V. (1997). 'Introduction,' in R. V. Clarke (ed.) *Situational Crime Prevention: Successful Case Studies*. Second edition. Albany, NY: Harrow and Heston Publishers: 1 – 43.
[111] *Ibid:* 18.
[112] Clarke, R. V. & G. R. Newman (2006). *Outsmarting the Terrorists*. Praeger Security International.
[113] Newman, G. R. & R. V. Clarke (2003). *Superhighway Robbery: Preventing e-commerce crime*. Willian Publishing.
[114] Newman, G. R. (2009). Policy Thoughts on "Bounded rationality of identity thieves." *Criminology & Public Policy*, Vol. 8 (2): 275.

1.3 Approach

The charm of situational crime prevention as an approach and a theory is the fact that it is not bound by any particular discipline. As Newman and Clarke note, "[i]t focuses on situations, which, depending on where they arise, are best understood from many different perspectives."[115] As a result, the theoretical framework can be combined with an approach from another discipline. Before describing the specific methodological background developed to answer the central research question, the introduction of a classification scheme is necessary. This classification scheme is indispensable to provide a clear order for the search of facilitating factors in a more manageable way. These factors can be derived from a number of classifications, such as technical, organizational, and legal. This type of classification appears to be a popular scheme; yet, for this research I propose a different type of classification, which shall incorporate all of these aspects but approach them from an actor-centered perspective. The actors included as objects of analysis are the state both as protector and provider, financial service providers, consumers, and a small selection of others including internet service providers, money mules, data brokers, etc. This perspective also takes into consideration the *interests* of the actors which assists in the establishment of a background for the facilitating factors developed in the opportunity structure of financial identity theft. These interests must be analyzed alongside, or perhaps as part of, the opportunity structure in an effort to develop a realistic perspective on the room for improvement with regard to (existing) countermeasures. Parallel to the classification scheme runs the distinction between the facilitation of the first and the second stage. As indicated in the introduction, financial identity theft can be separated into a first and a second stage, which are facilited in different ways. This distinction runs through the research as a red thread and often remains implicit rather than explicit.

This study carries a comparative nature through the inclusion of the United States and the Netherlands. The decision to conduct a comparative study rather than a single case study rests in the ability to derive scientific and societal value from the different experiences held by both countries. The selection of the United States as an object of analysis is self-evident due to its vast experience with the problem of financial identity theft. This experience has led to the accumulation of a significant amount of information which allows the United States to serve as a guide for the exploration of financial identity theft in other countries. The selection of the Netherlands as the second case is based primarily on the necessity for academic research to determine the validity to previous warnings about the potential for financial identity theft to evolve into a major social problem. The structural comparison then between the United States and the Netherlands can contribute to an assessment focused on whether financial identity theft is a viable threat to Dutch society. This comparison deviates from the best known and still dominant variant of the comparative method which is controlled comparison.[116] Alexander L. George and Andrew Bennett describe controlled comparison as "…the study of two or more instances of a well-specified phenomenon that

[115] Newman & Clarke (2003): 24.
[116] George, A. L. & A. Bennett (2005). *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press.

resemble each other in every respect but one."[117] Despite the considerable appeal of controlled comparison, especially due to its resemblance of a scientific experiment, its application is difficult to accomplish. As an alternative to controlled comparison, George and Bennett identify within-case analysis. This type of analysis steers away from the 'variable-oriented' approaches, as Charles Ragin has labelled them, and instead turns to a more holistic approach of single cases.[118] As George and Bennet describe, "[t]his alternative approach focuses not on the analysis of variables across cases, but on the causal path of a single case."[119] These within-case analyses can nevertheless be used for cross-case comparisons on a small scale, as occurs in this study, which limits itself to two cases. This limitation is vital in an effort to ensure both cases receive sufficient attention and in-depth analysis in order to increase the value of the conclusions. More cases shall lead to a more superficial treatment of the material which inherently defeats the approach used within this dissertation.

To accomplish a within-case analysis, George and Bennett identify two distinct methods: the congruence and the process-tracing method. "The essential characteristic of the congruence method", George and Bennett note, "is that the investigator begins with a theory and then attempts to assess its ability to explain or predict the outcome in a particular case."[120] In the congruence method, the investigator does not have to trace the 'causal process' which leads the independent to the dependent variable. This is the main difference with the process-tracing method, which "…attempts to identify the intervening causal process—the causal chain and causal mechanism—between an independent variable (or variables) and the outcome of the dependent variable."[121] Since the main aim of this study is to identify the intervening 'causal' process, the latter method seems most appropriate. This is also due to the recognition of process-tracing as "…a methodology well-suited for testing theories in a world marked by multiple interaction effects, where it is difficult to explain outcomes in terms of two or three independent variables—precisely the world that more and more scientists believe we confront."[122]

This identification of 'causal' or rather facilitation processes occurs across two dimensions. The first dimension is the identification of the connection between the presence of facilitating factors and the occurrence of financial identity theft. This coincides with the primary aim of the situational crime prevention approach to analyze the situational conditions which facilite the commission of a specific crime. As shall became clear in the section below on limitations, it is difficult to factually determine how an incident of financial identity theft occurs. Even so, in abstract terms there is an awareness of how perpetrators of financial identity theft aim to accomplish the crime. This is precisely where the distinction between the first (the collection of personal information or instruments) and the second stage (the misuse of such information or instruments for financial gain) returns to serve as a guiding principle through the research of facilitating factors.

The second dimension traces the causal process of how such facilitating factors came into existence in the first place. This historical analysis on the

---

[117] *Ibid:* 151.
[118] To avoid confusion, a case here refers to a country.
[119] *Ibid:* 179.
[120] *Ibid:* 181.
[121] *Ibid:* 206.
[122] Hall qtd. in *Ibid:* 206.

background of facilitating factors is essential to place both the factors specifically and the opportunity structure generally in their proper context. The situational conditions which may facilitate financial identity theft also play other, often more positive, roles in contemporary society which must be borne in mind when reflecting upon the introduction of potential countermeasures.

To carry out the method of process-tracing, this study primarily relies on publicly available documents, including both primary and secondary sources. In particular for the Netherlands, the study shall also rely on a select number of interviews to complement the available documentation. The interviews primarily serve an exploratory function to guide the research and gain background information about relevant developments.

1.4 Limitations

To avoid misguided expectations from the start, several limitations are in order. Due to the lack of empirical information, especially in the Netherlands, on cases of financial identity theft, much of the research remains in the hypothetical arena. To some extent, this limitation is a more general restriction on academic research conducted on the topic of financial identity theft since the establishment of a causal process is difficult to accomplish due to the diverse modus operandi incorporated by perpetrators of the crime.

Besides the limitation introduced as a result of the lack of empirical information on actual incidents of financial identity theft, the rapid developments in the field also offer complications. Financial identity theft is very much a fluid topic. During the writing of this dissertation, several aspects changed which made certain conclusions obsolete or irrelevant. This research project was finalized on June 1, 2010 and as such only incorporated developments after this date in an ad-hoc manner.

Other limitations concern the air of secrecy surrounding the topic of financial identity theft, for especially the financial services industry remains hesitant to release information out of fear of reputation damage or the loss of consumer trust in the more advanced methods of payment. This complicates the development of a comprehensive story about the facilitation of financial identity theft in both the United States and the Netherlands.

1.5 Roadmap for Readers

This book commences its journey through a chapter on definitional dilemmas introduced as a result of the introduction of the concept of identity theft into contemporary society. This chapter sets the tone for the versatile and complicated nature of identity theft and therefore sets the stage for the remainder of the book. After the chapter on definitional dilemmas, each actor is individually analyzed based on its contribution to the opportunity structure of financial identity theft. Chapter 3 analyzes the connection between the state as protector of the people and financial identity theft. This chapter mainly reviews the countermeasures either in place or introduced to combat identity theft, and as such maintains a different character from the other chapters. Chapter 4 reviews the state as provider. As provider, the government establishes an identification infrastructure which both the public and the private sector use to identify citizens and clients alike. Chapter 5 turns to the industry of financial services and evaluates the role

played by financial service providers, consumer reporting agencies, and financial supervisory organs in the potential facilitation of financial identity theft. Chapter 6 provides an overview of the role played by consumers as facilitators, but the chapter also reflects in a more critical manner on the ongoing debate about the ability and the responsibility of consumers to reduce the risk of financial identity theft. Chapter 7 observes the potential facilitation of other actors, including information brokers, payment processors, merchants, Internet Service Providers, and money mules. In conclusion, chapter 8 develops an overarching opportunity structure for financial identity theft based on the previous chapters and also reflects on existing countermeasures based on the opportunity reduction techniques set forth in the situational crime prevention framework.

2 | Definitional Dilemmas

The introduction of identity theft into contemporary society caused considerable conceptual confusion. The mere terminology became the source of vivid discussions, especially since individuals with a legal background questioned the usage of the word 'theft' in association with identity. The main question from the legal front became: can someone *steal* an identity? Traditional definitions of theft in criminal law conflicted with the meaning of the term as used in the concept of identity theft. Certain sources labelled identity theft therefore a misnomer[123] or refer to the concept as 'awkward.'[124] Some even demonstrate a complete disdain for the term.[125] Others, on the other hand, embrace the concept and its accuracy.[126] Clare Sullivan supports the usage of the concept of identity theft and states "[d]ishonest use of an individual's token identity by another person is a denial of the individual's right to the exclusive use of his/her transactional identity, and its use by another person fundamentally damages the integrity of the individual's token identity."[127] The acceptance of identity theft as a concept requires a stretch of the term theft and also a more progressive approach to the idea of property, which is a considerable challenge due to traditional meanings in the legal arena.[128] The availability of a popular alternative—identity fraud—provides those opposed to the use of identity theft as a concept an opportunity to circumvent the problem.[129] Even so, the problems associated with the usage of identity theft as a concept only proved to be the proverbial tip of the iceberg. The much larger challenge remains. This is the challenge of the problem definition. To address this challenge, this chapter shifts the discussion from the 'legal' to the

---

[123] The Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General (2008: 14) states in its *Final Report Identity Crime*, "[t]he phrase 'identity theft' is a misnomer, as identity theft does not actually deprive a person of their identity. The offence of theft or larceny traditionally involves an appropriation of the personal property of another with the intention to deprive him or her of that property permanently. Wrongfully accessing or using a person's personal information or forging proof of identity documents, without taking any physical document or thing, would not deprive the person of the ability to use that information."

[124] Koops, E. J. & R. E. Leenes (2006: 5) write how "'[i]dentity theft' is a rather awkward term, since identity is not something that is typically stolen. A characteristic of theft, after all, is that the owner no longer possesses the stolen thing. With identity, this is usually not the case: the victim of identity takeover still retains her identity. We should therefore speak of 'identity "theft"' rather than of 'identity theft.'"

[125] James Van Dyke, President and Founder of Javelin Strategy & Research, published a blog entry on April 14, 2010 with the title "'Identity theft': the sooner this term goes away the faster we'll make the problem do the same." In the post, he states "I've long disdained the term 'identity theft', but because it's stranglehold on the untapped power of higher understanding is supported by the highest laws of the land (the last two presidents have created 'identity theft task forces' and every federal, state and local law enforcement agency uses this same label) it won't disappear anytime soon."

[126] See for example Le Lievre, E. & R. Jamieson (2005: 7) who note how despite the difficulty with regard to criminal law aspects identity theft has more of a personal emotive impact than identity fraud because it presents the idea of identity ownership which is then stolen by another individual.

[127] Sullivan, C. (2009). Is Identity Theft Really Theft? *International Review of Law, Computers, and Technology*, Vol. 23: 85.

[128] This challenge maintains a more extensive history through the discussion of data as property. See Prins, J. E. J. (2006). 'Property and Privacy: European Perspectives and the Commodification of Our Identity,' in L. Guibault & P. B. Hugenholtz (eds.), *The Future of the Public Domain*, Kluwer Law International: 223 – 257.

[129] Identity theft and identity fraud are used both interchangeably by some and as separate concepts by others.

public policy arena in an effort to develop a more thorough understanding of the definitional dilemmas. This shift of arena provides for a more comprehensive approach to the issue of problem definitions since it surpasses the rigidity of legal debate.

2.1 Problem Definition

The importance of problem definitions in the development of public policy is evident through the attention devoted to the topic. Problem definitions play a prominent role in the shaping of political agendas and their substance therefore often become the focus of extensive debate.[130] David A. Rochefort and Roger W. Cobb describe how "[a]s political discourse, the function of problem definition is at once to explain, to describe, to recommend, and, above all, to persuade."[131] These different functions of problem definitions heighten the pressure on those involved to ensure their interests are reflected in the problem definition used during policy debates. Janet A. Weiss specifically emphasizes the aspect of persuasion of the problem definition when she writes, "...participants in the policy process seek to impose their preferred definitions on problems throughout the policy process. Much policymaking, in fact, is preoccupied with whose definitions shall prevail."[132] To successfully persuade others to accept a definition also grants the persuader the power to play a prominent role in the determination of the subsequent course of action with regard to the problem. This is because "[p]roblem definition is a process of image making, where the images have to do fundamentally with attributing cause, blame, and responsibility."[133] The causes reflected by the definition assist in the distribution of blame and responsibility. Rochefort and Cobb therefore consider culpability the most prominent aspect of problem definitions.[134] Even so, Rochefort and Cobb do acknowledge how "...problem definition is about much more than just finding someone or something to blame. Further disputes can surround a situation's perceived social significance, meaning, implications, and urgency. By dramatizing or downplaying the problem and by declaring what is at stake, these descriptions help to push an issue onto the frontburner of policymaking or result in officials' stubborn inaction and neglect."[135] This theoretical background assists in the development of an understanding of the discussions about the problem definition with respect to identity theft. Moreover, such an understanding also places the responses to the problem in perspective.

2.2 The Search for a Definition

The preoccupation with a definition of identity theft 'officially' began in 1998 when the Government Accountability Office (GAO) of the United States

---

[130] Rochefort, D. A. & R. W. Cobb (1994). 'Problem Definition: An Emerging Perspective,' in D. A. Rochefort & R. W. Cobb (eds.) *The Politics of Problem Definition: Shaping the Policy Agenda*. University Press of Kansas.
[131] *Ibid:* 15.
[132] Weiss, J. A. (1989). The powers of problem definition: The case of government paperwork. *Policy Sciences*, Vol. 22: 98.
[133] Stone, D. A. (1989). Causal Stories and the Formation of Policy Agendas. *Political Science Quarterly*, Vol. 104 (2): 282.
[134] Rochefort & Cobb (1994): 15.
[135] *Ibid:* 3.

identified the lack of a standard definition of the problem on several occasions.[136] The GAO literally states how "[t]here is no one universally accepted definition of identity fraud."[137] This conclusion appears based in part on testimonials provided by officials from the law enforcement community[138] as well as the credit card industry.[139] Michael D. White and Christopher Fisher identify the inconsistency in defining the problem as the primary challenge in the fight against identity theft.[140] Despite the introduction of a legal definition of identity theft, through the Identity Theft Assumption and Deterrence Act of 1998,[141] the United States Department of Treasury highlighted the definition problem in 2005 and wrote, "[t]he lack of a standard definition makes it difficult to collect comprehensive, accurate data for quantifying the costs and incidents of identity theft."[142] The Department cites various examples, mainly from the financial services sector which demonstrate the discrepancy among definitions used in the United States. Identity theft, according to the Department, is a definition in progress for certain sources in the financial services sector.[143]

Along similar lines, the Fraud Prevention Expert Group (FPEG) of the European Commission writes, "[t]he first difficulty is to define the scope of the problem as there is no clear common definition of what should be understood by identity theft or identity fraud."[144] Such a "...common definition of what the problem is appears desirable: talking of the same thing facilitates preventing and combating it."[145] Despite the importance granted to the issue, the FPEG notes how "[f]or the purposes of this paper, however, no attempt to find a common definition will be undertaken. The problem will be referred to as 'identity theft/fraud.'"[146]

The Organisation for Economic Co-operation and Development (OECD) also states how there is a lack of a common definition among OECD countries which "...may complicate efforts to combat the problem in a comprehensive, cross-border fashion."[147] Further along, the OECD once again notes the lack of a common definition and its potential to "…stymie efforts to address the problem."[148] The Australasian Centre for Policing Research (ACPR) describes the need to establish "...some form of consensus in relation to definitions of identity

---

[136] General Accounting Office (GAO) (1998). *Identity Fraud. Information on Prevalence, Cost, and Internet Impact is Limited*. Briefing Report to Congressional Requesters.
[137] *Ibid:* 11.
[138] The GAO (1998: 20) states how, "[i]dentity fraud is difficult to track. Generally, the law enforcement officials we contacted told us that their respective agencies historically have not tracked identity fraud for various reasons. One reason is the lack of a standardized definition of identity fraud."
[139] The GAO (1998: 43) states how, "[a]ccording to an official we contacted at VISA U.S.A., Inc., within the credit-card business, there is no standardized or industrywide definition of identity fraud."
[140] White, M. D. & C. Fisher (2008). Assessing Our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Efforts. *Criminal Justice Policy Review*, Vol. 19 (1): 3 – 24.
[141] Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007 (1998) (amending 18 U.S.C. § 1028).
[142] United States Department of Treasury (2005). *The Use of Technology to Combat Identity Theft*. Report on the Study Conducted Pursuant to Section 157 of the Fair and Accurate Credit Transactions Act of 2003.
[143] *Ibid:* 7.
[144] Fraud Prevention Expert Group (FPEG) (2007). *Report on Identity Theft/Fraud*: 8.
[145] *Ibid.*
[146] *Ibid.*
[147] Organisation of Economic Co-Operation and Development (OECD) (2009). *Online Identity Theft*, OECD Publishing: 9.
[148] *Ibid.*

crime terms, at least within Australasian law enforcement and revenue protection agencies, to assist with:

- ✓ policy development;
- ✓ Research;
- ✓ Training;
- ✓ Marketing and community education;
- ✓ Victim assistance measures;
- ✓ The treatment and measurement of this phenomenon; and
- ✓ The eventual development of comparable national statistics."[149]

The Ministry of Justice in the Netherlands also underscored the need for a demarcation of the concept of identity theft. This decision came as a result of the written commitment made by the Minister of Justice in 2004 to develop a policy framework in response to identity theft after the Royal Constabulary published a study on identity theft and travel documents.[150] Part of the development of such a policy framework was a workable demarcation of the problem of identity theft. This led to a study in 2007, which aimed to provide the government with a definition of the problem and an analysis of the applicability of existing instruments of criminal law.[151]

Through a comprehensive overview of the available literature and the various perspectives, the researchers needed to determine whether identity theft required a separate legal provision. Bald de Vries *et al.* provide an overview of definitions set forth in the Netherlands, the United States, the United Kingdom, France, Belgium, and the European Union. The exclusion of Australia is remarkable due to the availability of and the effort made by certain actors to create a more consistent approach toward a definition of identity theft, as noted above. Even so, the report produced by de Vries *et al.* is substantial[152] and provides a thorough dissection of all the definitions discussed. In their report, de Vries *et al.* propose the following definition of identity *fraud*. According to the researchers, "[i]dentity fraud is obtaining, taking, possessing or creating false means of identification intentionally (and) (unlawfully or without permission) and to commit with them unlawful behavior or: to have the intention to commit unlawful behavior."[153] Important to note is how the usage of false means of identification in the definition refers to means of identification "…when they do not truthfully identify the person who uses it."[154] The value of the study is difficult to determine for the definition set forth by the authors fails to surface in discussions on the topic.[155] On a different dimension, the Ministry of Justice used the results to strengthen its decision not to criminalize identity theft for the foreseeable future (see section

---

[149] Australasian Center for Policing Research (ACPR) (2006): 13.
[150] Koninklijke Marechaussee (2003). *Rapport identiteitsfraude en (reis)documenten*.
[151] De Vries, U. R. M. Th., Tigchelaar, H., van der Linden, M. & A. M. Hol (2007). *Identiteitsfraude: Een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen.* Wetenschappelijk Onderzoek en Documentatie Centrum (WODC).
[152] 270 pages.
[153] *Ibid*: 18.
[154] *Ibid*.
[155] Representatives from the consumer complaint center and the expert center for identity theft described how they used the definition as a (rough) guideline. Otherwise, the definition seems to not have been embraced in the policy debate in the Netherlands.

3.1.2). The definition also became the object of criticism, albeit limited.[156] There is merit to such criticism for the outcome of the study fails to surpass previous attempts and as such makes little to no contribution to the discussion.

Other academic attempts do manage to successfully accomplish such progress. Bert-Jaap Koops & Ronald E. Leenes defined identity theft as "…fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool without that person's consent."[157] There is a simplicity to the definition which is absent in the definition provided by de Vries *et al.* This simplicity embodies the craving for a broad range of the concept. As John Gerring notes, "[a] concept that applies broadly is more useful than a concept with only a narrow range of application. A good concept stretches comfortably over many contexts; a poor concept, by contrast, is parochial – limited to a small linguistic turf."[158] Other academic contributions to the discussion on definitions are more specific for these contributions focus on the highly contested definition of financial identity theft (see section 2.3).

From the above, it becomes obvious how a general consensus exists about the lack of a standard definition of identity theft. This is partly a result of the versatile nature of identity theft. The connection between identity theft and other crimes demonstrates this versatility and supports the complexity of the problem. Individuals misuse identities, whether real or fabricated, in an effort to carry out acts of terrorism, illegal immigration, human trafficking, and money laundering. The connection between identity theft and these other categories of crime challenges the establishment of policy ownership. As Joseph R. Gusfield notes, "[o]wnership constitutes one piece of the structure of public problems. It indicates the power to define and describe the problem."[159] This power is not clearly delineated with respect to identity theft due to the lack of explicit policy ownership.

Another part of the complexity is the 'novel' character of the problem. Whereas disagreements exist about the novel character of the phenomenon, many contend the incorporation of digital technology certainly provided the phenomenon with innovative aspects which make the overall problem display a sense of novelty. Rochefort and Cobb identify the aspect of novelty in relation to problem definitions and describe how "...issues that have not been seen before are difficult to conceptualize and they lack familiar solutions. Thus a tension arises as the issue is publicized and onlookers expect resolution, yet no consensus exists within the political system on how to tackle the problem."[160] This observation made by Rochefort and Cobb is particularly important in light of the continued emphasis on the lack of a standard definition.

---

[156] In an epilogue to his Master thesis, Peter van Schijndel reflects on the research conducted and the conclusions offered by de Vries *et al.* Van Schijndel recognizes the comprehensive character of the research conducted, but refutes the conclusions drawn by the authors. He even considers the potential acceptance and subsequent implementation of the definition by the Ministry of Justice dangerous. The definition set forth by de Vries *et al.* is, according to van Schijndel, a poor imitation or a bad copy of the definition presented by the Identity Theft Assumption and Deterrence Act of 1998 in the United States.

[157] Koops, E. J. & R. E. Leenes (2006). ID Theft, ID Fraud and/or ID-related Crime. Definitions matter. *Datenschutz und Datensicherheit*, Vol. 30 (9): 553-556.

[158] Gerring, J. (2001) *Social Science Methodology: A Criterial Framework*. Cambridge University Press: 54.

[159] Gusfield, J. R. (1981). *The Culture of Public Problems: Drinking-Driving and the Symbolic Order*. Chicago: University of Chicago Press: 13.

[160] Rochefort & Cobb (1994): 21.

When the GAO identified the lack of a standard definition in 1998, this seemed logical due to the 'novelty' of the problem. More than ten years later, the preoccupation with the lack of a standard definition might demonstrate a lack of consensus about the approach to the problem rather than the problem itself. Julia S. Cheney remarks how "[a]fter much discussion, Lois Greisman, of the FTC, suggested that perhaps the definitional debate is not the real roadblock, and in fact, such debate may be primarily about semantics."[161] The 'real roadblock' concerns the approach to the problem, which might be the underlying reason reflected in the statements made about the lack of a standard definition. This observation also receives support from the discrepancy between the reiteration of the absence of a definition despite considerable efforts made by the academic community to clarify the meaning of the concept and its related terminology.[162]

2.3 Financial Identity Theft

Since the focus of this research is on financial identity theft, this section shall concentrate on the problem definition issues specifically related to financial identity theft. Unlike the previous sections, which demonstrate how many sources emphasize the absence of a definition or a general consensus about the meaning of the concept, the definitional challenges of financial identity theft are more concrete. These challenges mainly originate from the distinct interest of the relevant parties, including governments, especially the law enforcement community, financial service providers, and in more limited capacity interest groups. The problem definition of financial identity theft is of vital importance for financial service providers, especially since the definition provides a reflection of causation and responsibility. The starting point for the United States is the legal definition established through ITADA, which states that identity theft occurs when someone "…knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."[163] This definition takes a comprehensive approach to identity theft in general and therefore includes various types of fraud.[164]

Such a broad definition became an object of resistance for the financial services industry after the passage of the Fair and Accurate Credit Transactions Act in 2003, when the Federal Trade Commission (FTC) received the opportunity to establish, among other things, identity theft definitions.[165] Whereas ITADA established a criminal definition of identity theft in 1998, the FTC needed to

---

[161] Cheney, J. S. (2005). Do Definitions Still Matter? Discussion Paper Payment Cards Center, *Federal Reserve Bank of Philadelphia*, p. 9.

[162] See for example Sproule, S. & N. Archer (2006). *Defining Identity Theft – A Discussion Paper*. Prepared for the Ontario Research Network in Electronic Commerce (ORNEC) Identity Theft Research Program; Koops, E. J., Leenes, R. E., Meints, M., Meulen, N. S. van der, & Jaquet-Chiffelle, D. O. (2009). A typology of identity-related crime: Conceptual, technical, and legal issues. *Information, communication & society*, Vol. 13(1): 1-24.

[163] Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007 (1998) (amending 18 U.S.C. § 1028).

[164] Cheney (2005).

[165] FACTA states in Sec. 111(3) how "[t]he term 'identity theft' means a fraud committed using the identifying information of another person, subject to such further definition as the Commission may prescribe, by regulation."

establish civil definitions of identity theft as a result of FACTA in 2003. The definition set forth by the FTC embraced the previously identified broad character. As such the FTC defined identity theft in its final rule as "…a fraud committed or attempted using the identifying information of another person without authority."[166] The definition set forth by the FTC is the result of the Commission's intent to cover "…all bona fide victims and conduct..."[167]

The financial services industry offered its disapproval through its comments on the proposed rule and the definition therein. The disapproval concerned the broad character of the definition and especially the inclusion of attempted fraud. Wells Fargo & Company expressed its dissatisfaction with the definition and wrote, "[w]e are concerned that defining 'identity theft' to include 'attempted' fraud would greatly expand the scope of conduct that entities must take steps to prevent and would significantly increase the number of consumers authorized to take advantage of the rights that the FCRA confers upon identity theft victims."[168] Furthermore, by "[e]xpanding the definition of identity theft beyond the traditional notion of an individual opening an account or obtaining a loan in another person's name would divert significant resources away from actual identity theft and its victims in order to assist those who have avoided any meaningful harm of identity theft."[169] Here the issue is mainly the inclusion of account takeover as part of the definition which also concerns others who claim how the broad definition leads to a dilution of the industry's efforts because such a definition provides victims of account takeover with the same benefits and priority as victims of true identity theft.[170] Such a dilution of efforts is unbeneficial to victims of 'true' identity theft since they fail to receive a higher priority in comparison to victims of 'less debilitating crimes' such as account takeover. This assertion of account takeover as a less debilitating crime is (highly) subjective since such a crime can still contain the necessary consequences for the victim, especially if such a takeover concerns a checking or savings account which may leave the individual (temporarily) without any funds.

Overall, Julia S. Cheney summarizes the position of the financial services industry when she writes, "[t]o optimize strategies to combat identity theft, the industry wants more nuanced definitions as determined by the specific form of fraud and by the process used to identify and respond to its losses and its customers."[171] The 'nuanced', or better yet restricted or limited, definitions therefore serve as tools for strategy optimization. This could be because more restrictive definitions limit their applicability to particular products within the sector of financial services. As Rodger Jamieson *et al.* note, "[p]rivate organisations interviewed saw identity fraud, identity theft and identity deception acts in much narrower focused terms than government agencies."[172]

The specificity of the form of fraud is also important in the Netherlands, where the Dutch Banking Association described how banks categorize fraud

---

[166] Federal Trade Commission (FTC) (2004). Final Rule. Available at: http://www.ftc.gov/os/2004/10/041029idtheftdefsfrn.pdf (last accessed July 4, 2010).
[167] *Ibid.*
[168] *Ibid:* 8.
[169] *Ibid.*
[170] *Ibid:* 10.
[171] Cheney (2005): 3.
[172] Jamieson, R., Sarre, R., Steel, A. & G. Stephens (2008). Defining Identity Crimes. Paper presented at the *19th Australasian Conference on Information Systems*, 3-5 December 2008 Christchurch. Available at: http://www.bsec.canterbury.ac.nz/acis2008/Papers/acis-0183-2008.pdf (last accessed July 4, 2010).

according to the specific type of 'product' involved.[173] Banks in the Netherlands therefore often speak of skimming[174] and Internet banking fraud, which clearly indicate which product perpetrators misused to obtain the victim's financial assets. This categorization occurs because different products reveal diverse vulnerabilities. Moreover, identity theft or the misuse of identities or identifying information is a common thread through most, if not all, types of fraud which take place in the banking industry.[175] The Dutch Central Bank therefore refers to the concept of identity theft as a *containerbegrip* or umbrella term.[176]

Still, the controversy witnessed about the term in the United States appears largely absent in the Netherlands with respect to the financial services sector. The National Forum on the Payment Systems reflects on the substance of identity theft and dissects the problem according to the stages identified in section 1.2. The Forum states how identity theft can be divided into two actions which include the acquisition and collection of information and the subsequent misuse of such information.[177] Whether the Forum also incorporates account takeover as part of this definition remains unclear, especially since the Forum, along with its participants, exclusively refer to specific types of or rather methods used to accomplish account takeover, such as skimming and phishing.[178]

Whereas the providers of financial services primarily frame their preference or need for more restricted and specific definitions in light of strategy optimization, others focus on ulterior motives held by the industry. As sergeant Ed Dadisho indicates, many financial service providers object to the usage of a broad definition by the FTC in particular and the government in general because such a definition "…*trigger certain duties* for the financial institutions, thereby allocating additional resources and system changes to respond to new identity theft complaints by consumers. This is purely a financial concern that would not merit any reason to change how law enforcement agencies report and investigate identity theft crimes."[179]

Moreover, the application of a broad definition carries the potential for unintended consequences, such as the development of unwarranted fears among consumers about the use of electronic payments and commerce.[180] Such unwarranted fears may occur as a result of the publication of statistical data on the problem. Fragmentation, or the publication of data based on specific banking products, circumvents this problem since such data makes the problem appear less dramatic. The Netherlands provides statistics specifically on skimming and on internet banking fraud. This exemplifies the fragmented approach.

---

[173] Interview February 9, 2010, Amsterdam.
[174] Skimming refers to the copying of the information on the black magnetic stripe on the back of a debit card in an effort to duplicate the card, obtain the pin code, and drain the account.
[175] Interview February 9, 2010, Amsterdam.
[176] Interview January 12, 2010, Amsterdam.
[177] Maatschappelijk Overleg Betalingsverkeer (2006). *Rapportage Maatschappelijk Overleg Betalingsverkeer 2005*.
[178] In the yearly report of the National Forum on the Payment System in 2007, there is no reference to identity theft. Instead, the report specifically highlights evolving problems with respect to skimming and phishing. See Maatschappelijk Overleg Betalingsverkeer (2008). *Rapportage Maatschappelijk Overleg Betalingsverkeer 2007*. Even so, the following year, the Forum once again referred to the problem of identity theft in its yearly report. See Maatschappelijk Overleg Betalingsverkeer (2009). *Rapportage Maatschappelijk Overleg Betalingsverkeer 2008*.
[179] Dadisho, E. (2005). Identity Theft and the Police Response: The Problem. *The Police Chief*, Vol. 72 (1).
[180] Cheney (2005)*:* 17.

In the United States, the publication of prevalence data by the FTC heightened the industry's concerns. Certain sources, including the American Bankers Association Senior Federal Counsel Nessa Feddis, claimed the figures associated with identity theft exaggerated the problem since all kinds of fraud were 'redefined' as identity theft.[181] The inclusion of all forms of unauthorized credit card use by the FTC also received criticism from Avivah Litan, a research director at Gartner, Inc. Litan describes how "[n]obody ever did it that way before."[182] This is rather peculiar given that the GAO published a study in 2002 and reported how "[t]he two major payment card associations, MasterCard and Visa, use very similar (although not identical) definitions regarding which categories of fraud constitute identity theft. Generally, the associations consider identity theft to consist of two fraud categories—account takeovers and fraudulent applications."[183] This appears to be contradictory since the conventional meaning of account takeover concerns the unauthorized use of existing credit cards. The explanation is concealed in a footnote where the GAO states, "[o]ther fraud categories that the associations do not consider to be identity theft-related include, for example, lost and stolen cards, never-received cards, counterfeit cards, and mail order/telephone order fraud."[184] The exclusion of all of these types of fraud leads to confusion about the payment association's definition of account takeover since many of the fraud categories mentioned in the footnote certainly fall under the account takeover umbrella. The inclusion of account takeover is a form of 'definition creep' which may lead to 'public confusion.' Rosie Lombardi claims how identity theft "...is now being used to sex up crimes reported in the media that were considered plain ordinary fraud in the past."[185] This is problematic for the industry since the more encompassing the definition of identity theft becomes the more prevalent the problem appears to be. As Stacey L. Schreft notes, lumping new account fraud together with existing account fraud makes identity theft appear more prevalent, which might raise more alarm among the public than financial service providers find necessary. Schreft furthermore writes, "[t]he latter argument, along with a desire of financial institutions to minimize the perceived prevalence and seriousness of the crime, is likely driving the objections to the ITADA's definition..."[186]

Whereas the financial services industry actively lobbies for a limited definition of financial identity theft, the government, especially law enforcement, continues to embrace a broad definition. Interest groups also express a preference for the usage of a broad definition. These interest groups represent the plight of victims of identity theft which enhances their preference for a broad definition in an effort to assist all victims rather than a selected group. The Identity Theft Resource Center (ITRC) in particular aims to capture the experiences of all types of victims of identity theft, including financial and criminal. For the victims of financial identity theft, the ITRC includes both victims of account takeover and true name

---

[181] O'Sullivan, O. (2004). ID Theft Overstated? Some Think So. *ABA Banking Journal*, Vol. 96: 8 – 9.
[182] *Ibid:* 8.
[183] General Accounting Office (2002). *Identity Theft: Prevalence and Cost Appear to be Growing.* Report to Congressional Requesters, GAO-02-363: 6.
[184] *Ibid.*
[185] Lombardi, R. (2006). Myths about identity theft debunked by experts. Available at: http://www.itworldcanada.com/news/myths-about-identity-theft-debunked-by-experts/98501 (last accessed July 4, 2010).
[186] Schreft, S. L. (2007). Risks of Identity Theft: Can the Market Protect the Payment System? *Economic Review*, Fourth Quarter: 7 – 8.

fraud. The ITRC demonstrates its inclusion of both forms of financial identity theft, when the interest group writes "[d]ue to the constant availability and exposure of financial account information and Social Security Numbers, it is relatively easy for an identity thief to either open new lines of credit or use/takeover existing accounts."[187] Along similar lines, the Electronic Privacy Information Center describes the many different types of identity theft on its website. For financial identity theft, the Electronic Privacy Information Center (EPIC) refers to credit card fraud as well as new account fraud.[188] The Privacy Rights Clearinghouse also captures both account takeover and application fraud as types of financial identity theft.[189] All three of the interest groups involved in consumer and victim advocacy demonstrate an all-encompassing approach to the problem of financial identity theft. This appears to be a logical result of their focus on consumers and victims of identity theft.

From the academic arena more fruitful efforts aim to develop an approach which provides both the specificity of the different aspects often grouped together as financial identity theft, but also maintains the umbrella perspective. Megan M. McNally provides a continuum of victimization which demonstrates the degrees of financial identity theft and the potential severity for its victims.[190] The continuum increases in terms of severity from left, existing accounts, to right, new activities. McNally places account takeover in the middle of her continuum. The left side of the continuum concerns fraudulent transactions on existing accounts which has as its worst case scenario account takeover. The right side of the continuum on the other hand reflects on the more serious form of financial identity theft, true name fraud. This continuum demonstrates how the definition of financial identity theft can be broad and nuanced simultaneously.

2.4 Conclusion

The treatment of the problem definition of identity theft in general and financial identity theft in particular sets the stage for its future in the realm of public policy. For many years, the main message has been that there is an absence of a standard or universally accepted definition of identity theft. This message is important, for its truth value is rarely questioned. Nor is the message about the need for such a standard definition ever challenged. As such, the definition of identity theft remains an object of preoccupation, despite the availability of academic literature which attempts to unravel its complexity. Even so, through maintaining the message of a lack of a standard definition, those involved managed to steer away from difficult choices. These choices must occur when they select a definition which inevitably identifies causes and distributes blame and responsibility. Not everyone in the arena is oblivious to this. In the minutes of the second meeting of the core group of experts on identity-related crime, the rapporteur notes how in relation to the discussion on definition, prevalence, and related matters "…Ozaki compared some of these issues to a 'chicken and egg' problem. Without

---

[187] Identity Theft Resource Center (2009). *Identity Theft: The Aftermath 2008*.
[188] Electronic Privacy Information Center (EPIC) (n.d.). Identity Theft. Available at: http://epic.org/privacy/idtheft/#Introduction (last accessed July 4, 2010).
[189] Privacy Rights Clearinghouse (2009). Fact Sheet 17: Coping with Identity Theft: Reducing the Risk of Fraud. Available at: http://www.privacyrights.org/fs/fs17-it.htm#crime (last accessed July 4, 2010).
[190] McNally, M. M. (2008). *Trial by Circumstance: Is Identity Theft a Modern-Day Moral Panic?* Dissertation Graduate School Newark Rutgers, the State University of New Jersey: 19.

legislation, there is no definitional basis for data gathering and an analysis and without data there was often no basis or perceived need for policy development and legislation."[191] As such, the reasoning remains circular and the absence of a definition functions as a vehicle to professionalize the art of procrastination. Interesting to note is how the minutes furthermore reflect on how Ozaki noted that the lack of a definition "…was not necessarily an insurmountable obstacle, however. There is no global definition of terrorism, but a reliable typology has been developed of some of the more problematic types, and international legal instruments, statistical analysis and technical assistance work had all been successfully carried out based on that typology."[192] This can be done for identity theft as well.[193]

Another reason to refute the preoccupation with the need for a standard definition of identity theft in an effort to respond to the problem is the (near) tradition of the existence of multiple definitions in the policy arena. Weiss notes, "[a]s policymakers struggle through the process of authoritative decision making, they typically face not only multiple options for addressing a given problem, but multiple definitions each implying its own family of solutions."[194] These multiple definitions, according to Weiss, "…may survive to haunt the implementation process..."[195] Therefore, while standard definitions may serve to optimize strategies they are not *required* to take action, unless such absence is a convenient justification to disguise the absence of ideas about how or a willingness or capacity to tackle the problem. Edgar A. Whitley and Ian R. Hosein write, "[g]iven this complexity in even identifying identity fraud, it is not immediately obvious which branch of government should be responsible for implementing measures for combating the problem."[196] And as such, the emphasis placed on the absence of a definition by stakeholders manages to postpone culpability and responsibility.

---

[191] Minutes of the second meeting of the core group of experts on identity-related crime, Vienna, Austria, 2-3 June 2008.

[192] *Ibid.*

[193] Koops, E. J., Leenes, R. E., Meints, M., Meulen, N. S. van der, & Jaquet-Chiffelle, D. O. (2009). A typology of identity-related crime: Conceptual, technical, and legal issues. *Information, communication & society*, Vol. 13 (1): 1 – 24.

[194] Weiss, J. A. (1989). The powers of problem definition: The case of government paperwork. *Policy Sciences*, Vol. 22: 98.

[195] *Ibid.*

[196] Whitley, E. A. & I. R. Hosein (2008). Departmental Influences on Policy Design. *Communications of the ACM*, Vol. 51 (5): 98.

3 | State as Protector

At its most fundamental level, the idea of the state as protector of the people can be traced back to Cicero's *salus populi suprema lex esto*, which translates into 'let the good of the people be the supreme law' or 'the welfare of the people shall be the supreme law.'[197] John Locke, in the *Second Treatise on Government*, cites Cicero's statement when he writes "*Salus populi suprema lex* is certainly so just and fundamental a rule, that he, who sincerely follows it, cannot dangerously err."[198] The role of protector, therefore, is often considered to be *the* fundamental function of government. Such protection can come about through various means. The diversity of means is in part a reflection of the variety of threats which people face in contemporary society. Simultaneously, such diversity is also a manifestation of the multi-faceted nature of the state, even in its function as protector of the people. For financial identity theft, this diversity is apparent, especially since identity theft is a versatile problem which implicates many different segments of the state. Throughout the literature on identity theft, nevertheless, certain aspects consistently return. Several sources discuss the legislative developments in the criminal law arena,[199] whereas others place an emphasis on data protection mechanisms in connection with identity theft.[200] Both of these elements of the state's effort to protect its people shall therefore receive extensive attention in this chapter. Furthermore, other sources also review the activities of the state as protector through its regulatory initiatives and supervisory organs with regard to business practices in connection to identity theft.[201] These shall receive considerable attention in chapter 5, where the financial services industry is discussed. The last part of this chapter focuses on diverse organizational features introduced to respond to aspects of identity theft, including its victims.

---

[197] Cicero, M. T. (44 BC). *De Legibus*. Book III.

[198] Locke, J. (1690). *Second Treatise on Government*. Chapter 13 Sec. 158.

[199] See for example Saunders, K. M. & B. Zucker (1999). Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act. *International Review of Law, Computers and Technology*, Vol. 13 (2): 183 – 192; Pastrikos, C. (2004). Identity Theft Statutes: Which will protect Americans the most? *Albany Law Review*, Vol. 67: 1137 – 1157; Sabol, M. A. (1999). The Identity Theft Assumption and Deterrence Act of 1998. Do individual victims finally get their day in court? *Loyola Consumer Law Review*, Vol. 11 (3): 165 – 173.

[200] See for example Solove, D. J. (2003). Identity theft, Privacy, and the Architecture of Vulnerability. *Hastings Law Journa*l, Vol. 54: 1227 - 1276; McKelvey, B. (2001). Financial Institutions' Duty of Confidentiality to Keep Customer's Personal Information Secure from the Threat of Identity Theft. *University of California Davis Law Review*, Vol. 34: 1077 - 1128; Shostack, A. & P. Syverson (2004). 'What Price Privacy? (and why identity theft is about neither identity nor theft),' in L. Jean Camp and S. Lewis, (eds.) *Economics of Information Security*. Norwell: Kluwer Academic: 129 - 142; McMahon, R. B. (2004). After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why is Identity Theft the Most Prevalent Crime in America? *Villanova Law Review*, Vol. 49: 625 – 660; Ludington, S. (2006). Reigning in the Data Traders: A Tort for the Misuse of Personal Information. *Maryland Law Review*, Vol. 66: 140 – 193.

[201] See for example Linnhoff, S. & J. Langenderfer (2004). Identity Theft Legislation: The Fair and Accurate Credit Transactions Act of 2003 and the Road Not Taken. *Journal of Consumer Affairs*, Vol. 38 (2): 204-216; Sovern, J. (2004). Stopping Identity Theft. *Journal of Consumer Affairs*, Vol. 38 (2): 233 – 243; Razvi, S. K. (2005). To What Extent Should State Legislatures Regulate Business Practices As a Means of Preventing Identity Theft? *Albany Law Journal of Science and Technology*, Vol. 15: 639-666.

3.1 Criminal Legislation

3.1.1 United States

When financial identity theft first surfaced in its current form in the United States, which was during the mid-nineties, many victim complaints fell on deaf ears with law enforcement officials. The law enforcement community did not recognize these individuals as crime victims, due to the lack of a specific legal provision which criminalized identity theft in general and financial identity theft in particular. Criminals proved to be acutely aware of this legal loophole. Robert Hartle, a victim of identity theft, testified before the United States Senate and described how "[i]t wasn't enough that this criminal stole my identity, but he actually called me on the phone and told me that there was not a law enforcement agency in the United States, not a police officer, not an FBI agent, nobody, not a judge, that would consider this crime as a crime against me."[202] Through his experiences, Hartle decided to use his situation to attract political attention to the fate of identity theft victims. He authored the Arizona State Law[203] which officially criminalized identity theft in the State of Arizona.[204] After drafting the bill, Hartle approached Arizona State Senator Tom Smith, who provided the necessary political assistance to get the bill passed and signed by the governor in 1996.[205] As a result, Arizona became the first State to pass such a provision and was later on followed by California[206], before other States joined the 'movement.'

After the successful action at the State level, Hartle continued his mission to criminalize identity theft at the Federal level and contacted Jon Kyl, a United States House of Representatives member from Arizona. Kyl, along with Congressman John Shadegg, worked endlessly, according to Hartle, to get the bill passed in Congress.[207] The introduction of the Identity Theft and Assumption Deterrence Act (ITADA) in 1998 became the ultimate reward for their hard work. ITADA states that an individual commits identity theft when he or she:

> "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."[208]

During the congressional hearing on the bill, Kyl proclaimed how "[w]hile the results of identity theft can be very costly for its victims, the law recognizes neither the victim nor the crime."[209] This remained the main argument in favor of a legal

---

[202] Hartle, R. (1998). Testimony to the U.S. Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary. *The Identity Theft and Assumption Deterrence Act*, Hearing, May 20, 1998 (Serial 105 - 779): 3.
[203] Arizona Criminal Code Revised Statute § 13-2008 (1996).
[204] Hartle, R. (2009). *Background*. Available at: http://www.idtheft.org/background.htm (last accessed July 4, 2010).
[205] *Ibid.*
[206] California Penal Code § 530.5
[207] Hartle (2009).
[208] Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007 (1998) (amending 18 U.S.C. § 1028).
[209] Kyl, J. (1998). Opening statement to the U.S. Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary. *The Identity Theft and Assumption Deterrence Act*, Hearing, May 20, 1998 (Serial 105 – 779): 1.

provision to officially criminalize identity theft. The introduction of ITADA successfully led to an increase in recognition for identity theft victims from the law enforcement community.[210] Kurt M. Saunders & Bruce Zucker call the previous lack of criminalization of identity theft surprising, especially since "[u]nder federal law, anyone who obtains, uses, or transfers false identification for the purpose of committing a fraudulent act without the consent of the holder of the identification commits a felony."[211] Yet, up until ITADA no federal statute criminalized the assumption of another person's identity without the involvement of false identification documents.

In addition to victim recognition, the law is also an attempt to align the legal landscape in the United States with society's advances. In contemporary society, false documentation is no longer a necessary condition to commit any type of identity theft, let alone financial identity theft. Instead, identification information alone became a convenient tool used by perpetrators to commit identity theft. Yet, such identification information did not receive protection under original criminal law. As Kyl stated, "[m]y bill recognizes technological advances by extending protection to identification information."[212]

Furthermore, the government also introduced the law to serve as a means of deterrence for future acts of identity theft. Perpetrators appeared rather well aware of the legal ambiguity of their actions. The phone call received by Hartle provides an exemplary indication of how his perpetrator knew about the lack of legal repercussions. The introduction of a separate criminal offense, as a result, also aimed to increase the risks for perpetrators engaged in identity theft. Deterrence, as an argument in defense of criminalization, however, remains a contested topic. As Miriam H. Baer notes, "[l]awmakers routinely invoke 'deterrence' as a reason for expanding criminal law, increasing penalties, or promising greater enforcement of white collar crimes. Scholars, however, have either downplayed or completely dismissed the value of deterrence theory for predicting, much less controlling, criminal conduct."[213] More specifically with regard to identity theft, Heith Copes and Lynne Vieraitis conducted interviews with incarcerated identity thieves in which they inquired about risk perception of the prisoners' actions.[214] Copes and Vieraitis conclude that most of the interviewed identity thieves devoted little thought to the possibility of getting caught. Those who did take such possibility into consideration deemed the actual risk low and the expected punishment to be minimal at most.[215] Certain interviewees indicated how the classification of identity theft as a white collar crime meant the risk of detection remains low and the potential punishment far from severe, at most a slap on the wrist.[216] As a

---

[210] Newman, G. R. & M. M. McNally (2005). *Identity Theft Literature Review*. Research report submitted to the United States Department of Justice. Available at: http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf (last accessed July 4, 2010).

[211] Saunders & Zucker (1999): 186.

[212] Kyl (1998): 1.

[213] Baer, M. H. (2008). Linkage and the Deterrence of Corporate Fraud. *Virginia Law Review*, Vol. 94: 1364.

[214] Copes, H. & L. Vieraitis (2007). *Identity Theft: Assessing Offenders' Strategies and Perceptions of Risk*. Research report submitted to the United States Department of Justice. Available at: http://www.ncjrs.gov/pdffiles1/nij/grants/219122.pdf (last accessed July 4, 2010). See also Copes, H. & L. Vieraitis (2009). Understanding Identity Theft: Offenders' Accounts of Their Lives and Crimes. *Criminal Justice Review*, Vol. 34: 329 – 349.

[215] *Ibid.*

[216] *Ibid.*

result, ITADA can be seen as more functional with regard to the victims than as a means of deterrence with respect to the perpetrators.[217]

Hartle's case along with the political assistance of both State and Federal representatives developed a policy window for political action. With Tom Smith at the State level and Jon Kyl at the Federal level as policy entrepreneurs, identity theft became an important topic on Washington's political agenda. John W. Kingdon speaks extensively about the role of policy entrepreneurs in *Agendas, Alternatives, and Public Policies*. In reference to Capitol Hill, he writes "[o]ne goal of a senator or representative is satisfying constituents. Publicity is essential, and one way to get publicity is to push for new policy initiatives."[218] Whereas policy entrepreneurs played a vital role in the introduction of ITADA, subsequent legislation benefited from the development of a different policy window.

Through the increased political momentum of the events of September 11, 2001, the United States Congress decided to introduce and subsequently pass additional legislation. In 2004, Congress passed the Identity Theft Penalty Enhancement Act (ITPEA), which outlines the issue of aggravated identity theft. ITPEA states that "[w]hoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years."[219] And that, "[w]hoever, during and in relation to any felony violation enumerated in section 2332b(g)(5)(B), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person or a false identification document shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 5 years."[220] The House of Representatives report describes how "[a]s international cooperation increases to combat terrorism, al-Qaida and other terrorist organizations increasingly turn to stolen identities to hide themselves from law enforcement."[221]

---

[217] Even when caught and convicted, only fifty per cent actually go to prison. See Rebovich, D. J. (2009). Examining Identity Theft: Empirical Explorations of the Offense and the Offender. *Victims & Offenders*, Vol. 4 (4): 357 — 364.

[218] Kingdon, J. (2003). *Agendas, Alternatives, and Public Policies*. New York: Longman: 41.

[219] Pub. L. 108-275, 118 Stat. 831-834. Subsection (c) states: "DEFINITION.—For purposes of this section, the term 'felony violation enumerated in subsection (c)' means any offense that is a felony violation of— "(1) section 641 (relating to theft of public money, property, or rewards), section 656 (relating to theft, embezzlement, or misapplication by bank officer or employee), or section 664 (relating to theft from employee benefit plans); "(2) section 911 (relating to false personation of citizenship); "(3) section 922(a)(6) (relating to false statements in connection with the acquisition of a firearm); "(4) any provision contained in this chapter (relating to fraud and false statements), other than this section or section 1028(a)(7); "(5) any provision contained in chapter 63 (relating to mail, bank, and wire fraud); "(6) any provision contained in chapter 69 (relating to nationality and citizenship); "(7) any provision contained in chapter 75 (relating to passports and visas); "(8) section 523 of the Gramm-Leach-Bliley Act (15 U.S.C. 6823) (relating to obtaining customer information by false pretenses); "(9) section 243 or 266 of the Immigration and Nationality Act (8 U.S.C. 1253 and 1306) (relating to willfully failing to leave the United States after deportation and creating a counterfeit alien registration card); "(10) any provision contained in chapter 8 of title II of the Immigration and Nationality Act (8 U.S.C. 1321 et seq.) (relating to various immigration offenses); or "(11) section 208, 811, 1107(b), 1128B(a), or 1632 of the Social Security Act (42 U.S.C. 408, 1011, 1307(b), 1320a–7b(a), and 1383a) (relating to false statements relating to programs under the Act)."

[220] Section 2332b(g)(5)(B) provides an extensive list to indicate what the Federal Crime of Terrorism as defined in Section 2332b(g)(5)(A) as "an offense that—is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct" is in violation of.

[221] Identity Theft Penalty Enhancement Act Report 108-528.

In addition to the fight against terrorism, the lack of deterrence capacity with respect to identity theft also became an incentive for the development of additional legislation. Under existing law, many perpetrators received either little or no prison time as a result of their actions. According to the report, such a lack of punishment became a tacit encouragement to those arrested to carry on such crimes.[222] The above discussion on the conclusions of Copes and Vieraitis on deterrence with respect to perpetrators of identity theft validates this concern. To strengthen its claim, the Report also cites various cases in which perpetrators received little or no prison time.[223] The Department of Justice, along with other government agencies, voiced strong support in favor of the Act. Yet, dissenters argued against the introduction of mandatory minimum sentences. During a Committee hearing, Scott states "[m]andatory minimum sentences not only defeat the rational sentencing system that Congress adopted, but make no sense in our separation of powers scheme of governance. Moreover, the notion that mandating a 2- or 5-year sentence to someone who is willing to risk a 15-year sentence already is not likely to add any deterrence."[224]

Whereas ITPEA in concept received considerable criticism, its application also became an object of controversy. The contentious nature of the Act and its application became the topic of a Supreme Court case in 2009. The case concerns the unlawful use of social security and alien registration numbers, which, unbeknownst to petitioner Flores-Figueroa, belonged to another individual. In 2000, Ignacio Flores-Figueroa, an illegal immigrant from Mexico, used, without lawful authority, a false social security and alien registration number to secure employment.[225] Flores-Figueroa also used a fabricated date of birth and provided his employer with a false alien registration card. Neither the social security nor the alien registration number belonged to a real individual. Several years later, in 2006, Flores-Figueroa wanted to use his real name and issued a different social security and alien registration number to his new employer. Flores-Figueroa provided alien registration and social security cards with his real name, but numbers which turned out to belong to actual individuals.[226] The employer handed the information over to the United States Immigration and Customs Enforcement office (ICE). ICE subsequently discovered that the numbers and the documents issued by Flores-Figueroa belonged to others. The discovery led the United States to charge Flores-Figueroa with two predicate crimes, namely, entering the United States without inspection, 8 U.S.C. §1325(a), and misusing immigration documents, 18 U.S.C. §1546(a).

Furthermore, the United States charged him with aggravated identity theft through ITPEA.[227] Flores-Figueroa requested a judgment of acquittal on the last charge, aggravated identity theft. In his motion, Flores-Figueroa claimed the government could not provide any evidence to demonstrate that he knew the numbers issued belong to real individuals. The government, in return, denied the need to prove such knowledge. The District Court, after a bench trial, accepted the argument set forth by the government to consequently convict Flores-Figueroa on the aggravated identity theft charge. Flores-Figueroa appealed, but the

---

[222] *Ibid:* 5.
[223] *Ibid.*
[224] *Ibid:* 27.
[225] *United States* v. *Flores-Figueroa* (U.S. Supreme Court No. 08-108, 2009).
[226] How the defendant obtained these numbers is not mentioned.
[227] 18 U.S.C. §1028A(a)(1))

Court of Appeals upheld the decision of the District Court.[228] The Supreme Court accepted the case due to the difference of opinions held among various courts in the past on this specific matter. Three court decisions[229] upheld the knowledge requirement, whereas three others[230] decided that the knowledge requirement in the Act did not apply to the element 'of another person.'

The Supreme Court unanimously voted in favor of the petitioner. In the Court's opinion, Justice Breyer writes "[t]here are strong textual reasons for rejecting the Government's position. As a matter of ordinary English grammar, it seems natural to read the statute's word 'knowingly' as applying to all the subsequently listed elements of the crime."[231] The government's main argument had been that the word 'knowingly' only applied to the verbs in the Statute and remained indifferent to the subject's knowledge of the object. Basically, the government claimed 'knowingly' applied to all but the last three words 'of another person.' From a grammatical point of view, the Court denied its claim. The Court therefore concluded the government needs to prove knowledge on the part of the petitioner. This was a requirement which the government failed to fulfil.

The government refers to another provision, section 2332b(g)(5)(B), within the Statute which specifically addresses perpetrators charged with terrorism as the predicate crime and goes beyond stating 'a means of identification of another person' and also lists 'or a false identification document.' Under this provision, Flores-Figueroa would have no claim. But 2332b(g)(5)(B) is not applicable, and 18 U.S.C. §1546(a) does not state anything about false documents. The text is clear for the Court; yet, Breyer takes a peek at the legislative history to go beyond the language in the Act. At least in one statement in the Report associated with the Act, identity theft and identity fraud are used interchangeably. Due to this interchangeable use of both terms, Breyer writes "[a]nd, in equating fraud and theft, Congress might have meant the statute to cover both—at least where the fraud takes the form of using an ID that (without the offender's knowledge) belongs to someone else."[232] This notion, however, is subsequently dismissed when Breyer notes how Congress clearly distinguishes 'the fraud crime' in 18 U.S.C. §1028 from 'the theft crime' in 18 U.S.C. §1028a. Accordingly, the knowledge requirement stands. This discussion of semantics which is inherent to the problem of identity theft (see chapter 2) overshadows the underlying issue of its victimization.

The Statute and its subsequent interpretation in judicial circles also influence other policy areas. Matthew T. Hovey claims how the pervasive issue surrounding the judiciary's decision on how the interpret ITPEA provides the United States Congress with a viable opportunity to implement immigration reforms.[233] Furthermore, Hovey claims how reading the Act in a way which requires the government to prove the defendant's knowledge of the authenticity of the numbers used for identification purposes renders ITPEA "...impotent in dealing

---

[228] *United States* v. *Flores-Figueroa* (8th Cir. 2008).
[229] *United States* v. *Godin*, 534 F. 3d 51 (CA1 2008); *United States* v. *Miranda-Lopez*, 532 F. 3d 1034 (CA9 2008); *United States* v. *Villanueva-Sotelo*, 515 F. 3d 1234 (CADC 2008).
[230] *United States* v. *Mendoza-Gonzalez*, 520 F. 3d 912 (CA8 2008); *United States* v. *Hurtado*, 508 F. 3d 603 (CA11 2007) *(per curiam)*; *United States* v. *Montejo*, 442 F. 3d 213 (CA4 2006).
[231] *United States* v. *Flores-Figueroa* (U.S. Supreme Court No. 08-108, 2009).
[232] *Ibid*: 9.
[233] Hovey, M. T. (2009). Comment: Oh, I'm sorry, did that identity belong to you? How ignorance, ambiguity, and identity theft create opportunity for immigration reform in the United States. *Villanova Law Review*, Vol. 54.

with the common situation of an illegal immigrant utilizing a random identification number or card that actually belongs to a real person."[234] While Hovey emphasizes the impact of identity theft on its victims, and therefore draws attention to a crucial aspect of the crime, he merely uses this element of the problem to further an argument against illegal immigration and the inability of Congress, according to him, to adequately respond to *that* problem. This virtually hijacks the core of identity theft and shifts the policy debate toward another issue. Such hijacking activities are rather typical for identity theft especially in its relation to other public policy issues, as becomes evident throughout the rest of the book.

Janice Kephart also criticizes the decision and proposes statutory language fixes in an effort to reverse the political implications of the Supreme Court decision. According to Kephart, the decision crippled the longstanding practice of prosecutors due to the requirement of proving the defendant knew the identification information belonged to another person. Kephart aims to demonstrate how the decision of the Supreme Court goes against congressional intent. While Kephart recognizes how "...nowhere in the House report is the issue addressed of whether a defendant has to 'know' his victim is a real person or not", she nevertheless claims "...it is clear that the House intended to widen the breadth of prosecutors' ability to vigorously pursue identity fraud."[235] Kephart draws this conclusion based on her interpretation of congressional intent, when she writes "...it seems relatively clear that a knowledge requirement of the victim was not intended, as that reading creates an outcome that inoculates some defendants and not others, which is clearly not what Congress was intending when it added mandatory sentencing guidelines designed to 'broaden the reach of' the identity theft statute."[236] This conclusion, nevertheless, remains based on her interpretation of the text rather than an explicit expression made by Congress. Just as Hovey, Kephart mainly ties her concern about the decision to the policy issue of immigration. She also refers to the victims of identity theft, but the main argument expresses a fear about the inability of prosecutors to fully prove their case due to a requirement which is difficult to adhere to due to the complexity of proving 'knowledge.'

The connection of illegal immigration returns when Kephart writes, "[w]hen illegal aliens use third parties to purchase ID documents or information, they should not be immune to a charge of aggravated identity theft. Fraudulent ID rings earn millions from criminals and illegal aliens whose only purpose in obtaining such documents is to misrepresent themselves and further assimilate into the United States. While the federal government works on these rings to bring them to justice, their clients — who knowingly buy their products — should not be let off the legal hook because they don't 'know' their victims."[237] To reverse the political implications of the decision, Kephart suggests the replacement 'of another person' with 'other than his own.' This eliminates the duty of the government to prove the defendant knew the information belonged to another person. Toward the end Kephart strengthens her case when she describes how Flores-Figueroa did not argue he did not know the information belonged to another person rather that the government was incapable of proving he knew.

---

[234] *Ibid:* 386.

[235] Kephart, J. (2010). Fixing Flores: Assuring Adequate Penalties for Identity Theft and Fraud. *Backgrounder,* Center for Immigation Studies: 6.

[236] *Ibid.*

[237] *Ibid:* 14.

This is crucial because this hurdle may be a recurring feature for public prosecutors in the future, which obviously creates apprehension for some since such a requirement renders the legislation less useful than anticipated or desired.

Even after the introduction of ITADA in 1998 and ITPEA in 2005, certain members of Congress continued to pursue identity theft legislation. Senator Patrick Leahy and Senator Arlen Specter introduced the Identity Theft Enforcement and Restitution Act of 2007 (S. 2168) in the Senate. During the floor speeches, Senator Leahy emphasized the need for better protection for American consumers. Through the introduced bill, Leahy and Specter primarily aimed to provide victims of identity theft with the ability to seek restitution for indirect costs incurred as a result of identity theft and especially the reparation of its consequences. Furthermore, Leahy and Specter wanted an expansion of the list of predicate offenses for aggravated identity theft. The Senators also wanted passing counterfeit securities, mail theft, and tax fraud to become predicate crimes. In addition, penalties awarded to convicted perpetrators of identity theft needed to become more severe and crime appropriate, according to the Senators.

While the bill passed in the Senate, its House of Representatives version (H.R. 6060 introduced by Adam Schiff) stranded in Committee. The proposal, however, became part of an omnibus bill[238] and found its way into law as a result shortly after. The Identity Theft Enforcement and Restitution Act of 2008 became part of the Former Vice President Protection Act, which President George W. Bush signed into law on September 26, 2008. The Act incorporated a selection of its original aspects. First, victims now have the ability to receive restitution for indirect costs incurred from the perpetrators of the crime. The Act states that an offender "…in the case of an offense under sections 1028(a)(7) or 1028A(a) of this title, pay an amount equal to the value of the time reasonably spent by the victim in an attempt to remediate the intended or actual harm incurred by the victim from the offense."[239] Among other things, the Act also issues a directive to the United States Sentencing Commission. The Act requests that the Sentencing Commission "…shall review its guidelines and policy statements applicable to persons convicted of offenses under sections 1028, 1028A, 1030, 2511, and 2701 of title 18, United States Code, and any other relevant provisions of law, in order to reflect the intent of Congress that such penalties be increased in comparison to those currently provided by such guidelines and policy statements."[240] Moreover, the Act states that "in determining its guidelines and policy statements on the appropriate sentence for the crimes enumerated in subsection (a), the United States Sentencing Commission shall consider the extent to which the guidelines and policy statements may or may not account for the following factors in order to create an effective deterrent to computer crime and the theft or misuse of personally identifiable data." [241] The Act outlines an extensive list of factors, which allows those who issue the sentence a great sense of liberty to increase the penalties for the crime. The likelihood of the inability to associate a factor listed in the Act with a specific incident of identity theft appears slim. The expansion of predicate offenses with regard to aggravated identity theft, as Leahy and Specter desired, however, failed to become part of the Act.

---

[238] Former Vice-President Protection Act of 2008. Pub. L. 110-326, 122 Stat. 3560-3565.
[239] *Ibid.*
[240] *Ibid.*
[241] See Sec. 209 (b).

3.1.2 The Netherlands

The historical background with regard to the topic of criminalization of identity theft in the Netherlands is less extensive and quite different in comparison to the United States. The topic of criminalization received attention from the Ministry of Justice in 2007 when the Ministry commissioned a study to establish a workable definition of identity theft and to examine whether additional legislation was needed with respect to identity theft (see section 2.2).[242] Based on the analysis of many definitions from various sources, the researchers turned to the correlation between the definitions and the available instruments of criminal law in the Netherlands. The relevant offenses in Dutch criminal law "…consist of so-called 'falsehood offences' (such as written falsehoods in documents, fraud with travel documents and payment cards), 'active and passive fraud', computer crimes, human trafficking and smuggling as well as theft, buying and selling stolen goods ('fencing'), embezzlement, general fraud ('oplichting'), and money laundering offences."[243]

The so-called 'falsehood offenses' are particularly relevant to identity theft when perpetrators falsify documents or alter authentic documents. These documents can be quite diverse including payment stubs, birth certificates, or other official documents, which are subsequently used to obtain financial benefits. Furthermore, criminal law in the Netherlands also specifically criminalizes fraud in connection with travel documents (which are official identification documents). This criminal offense is particularly relevant, according to the researchers, since many perpetrators of identity theft use travel documents as a 'source document' to continue their operations.[244] In the physical world this certainly appears likely, but in the digital world its importance becomes less relevant. In particular the connection between human trafficking and travel documents relates to this criminal offense. More relevant for this research project is the criminal offense which describes the falsification of bank and credit cards. This criminal offense responds to, for example, skimming activities of perpetrators.

Despite the availability of relevant criminal offenses which either respond to the first or the second stage of identity theft, the researchers still find particular gaps in the Dutch criminal law framework.[245] These gaps relate to 'horizontal fraud'[246] and in particular to the ability of perpetrators of identity theft to obtain services through the use of false or falsified personal data. With regard to specific criminalization of identity theft, the researchers emphasize the benefit of clarity which accompanies such an offense. Such clarity can increase the willingness to report and improve means of registration. This in turn can assist in the development of a more accurate picture of the problem and the necessary countermeasures, according to the researchers.[247]

After the publication of the study, discussions about the potential to introduce a separate criminal offense continued. The Ministry of Justice initiated expert

---

[242] De Vries, U. R. M. Th., Tigchelaar, H., van der Linden, M. & A. M. Hol (2007). *Identiteitsfraude: Een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen*. Den Haag: Wetenschappelijk Onderzoek en Documentatie Centrum (WODC).

[243] *Ibid:* 19.

[244] *Ibid.*

[245] *Ibid:* 260.

[246] Horizontal fraud refers to fraud between private parties, whereas vertical fraud concerns fraud between a citizen and the state.

[247] *Ibid.*

meetings in 2007 and 2008 to catalogue the diverse perspectives held by those involved. There is no publicly available documentation of these expert meetings and there is no genuine clarity on their impact on the decision making process. The following year, in 2009, the topic remained on the agenda and became more concrete through the delivery of two separate recommendations addressed to the Minister of Justice. Both of these recommendations are confidential. Insiders, however, were at liberty to disclose on a more abstract level how these recommendations described 'opposing viewpoints.' One recommendation stemmed in favor of a separate criminal offense, whereas the other opposed it.

In January 2010, the Minister decided to hold off on the criminalization of identity theft.[248] The Minister based his decision on the outcome of the WODC study cited above and another more policy oriented study conducted by the Directorate on Law Maintenance, Order and Crime Fighting (DRC). The WODC study, according the interpretation of the Ministry of Justice, did not indicate a legal necessity for additional legislation.[249] The DRC study provided similar conclusions with respect to the lack of necessity of additional legislation from a policy oriented perspective.[250] Moreover, there is no investigation priority and the current availability of legal instruments is deemed sufficient.

Overall, the Minister of Justice based his decision on the lack of immediate cause as reflected by other contextual developments.[251] These developments include the Minister's goal to amend article 231 of the Dutch Criminal Code (*Wetboek van Strafrecht*, hereafter: DCC) which concerns fraud with travel documents. This amendment to the article will expand the coverage of documents and as such surpass those previously mentioned in the article. The amendment includes all documents which individuals can use as identification documents to adhere to the identification obligation as listed in article 1 of the Identification Duty Act (*Wet op de identificatieplicht*). This amendment has as its primary goal to criminalize those who issue false or falsified identification documents and also those who purposefully use an authentic identification document of another person (the so-called look-a-like fraud).

With respect to identity theft on the digital highway, the DRC aims to monitor identity theft on the Internet. To accomplish this task, the Directorate aims to hold various expert meetings throughout 2010 with individuals from law enforcement agencies, the public prosecutor's office, and the academic arena. The Directorate also aims to incorporate the information available from a comparative study commissioned by the European Commission, which is being carried out in 2010. Simultaneously, the Council of Europe also plans to publish a discussion nota.

The European Commission alluded to criminalization several years ago in 2007 in its Communication 'Towards a general policy on the fight against cybercrime.'[252] In its Communication, the European Commission notes how "EU law enforcement cooperation would be better served were identity theft

---

[248] Director Instrumentation Procedures and Maintenance of Law and Order (2010). Letter to the Steering Committee of the Strengthening Identification in the Public Sector Program.
[249] Personal communication VIPS, June 1, 2010.
[250] *Ibid.*
[251] Director Instrumentation Procedures and Maintenance of Law and Order (2010).
[252] European Commission (2007). *Towards a general policy on the fight against cybercrime.* Communication from the Commission to the European Parliament, the Council and the Committee of Regions of 22 May 2007.

criminalized in all Member States."[253] The issue might be more complex than envisioned, however, since views within the European Union appear to be diverse. France, for example, rejected the introduction of additional legislation to criminalize identity theft.[254] Whilst the Minister of Justice in the Netherlands appears to be in anticipation of transnational and European developments, these may take longer than expected, especially since the discussion at the European level seems to have been (temporarily) postponed. The draft of the 18 month program issued for the Spanish, Belgian and Hungarian Presidencies do, however, refer to the issue of identity theft. The program specifically states "[i]dentification and recovery of criminal assets and the fight against money laundering will remain a key priority. The issue of identity fraud will be given particular attention and in this context, initiatives will be launched with regard to the verification of the authenticity of identity documents at the European level."[255]

Besides international developments, the Netherlands also passed an amendment in 2009 which concerns identity theft related activities. The Lower House passed an amendment to the criminalization of fraud in article 326 DCC.[256] The provision previously included fraudulently tricking persons into handing over data, but only data 'with monetary value in business transactions', i.e., on the legal market. This did not cover passwords, credit-card numbers, etcetera, which cannot be traded on the legal market. The amendment eliminated the part 'with monetary value in business transactions.' As a result, it now also criminalizes practices where individuals aim to obtain information, whether passwords, pin codes, or other valuable information, which in and of itself do not carry a monetary value in lawful business transactions. This amendment mainly appears to criminalize social engineering practices such as phishing.

Overall, the Minister believes how, in addition to the amendments listed above, good communication about the applicability of existing legislation can contribute to the prevention and suppression of identity theft. The Minister therefore recommends the development of a pamphlet which can assist law enforcement during the management of identity theft cases and its victims. This pamphlet will provide law enforcement with information on the relevant legislation in the DCC. The Ministry of Justice shall soon start with the development of this pamphlet. To develop a more comprehensive picture of the nature and prevalence of identity theft, an aspect which also receives attention during the discussions on criminalization, the Minister suggests the introduction of identity theft as a subcategory for the registration systems of law enforcement agencies.[257]

From an empirical point of view on identity theft, the information on the experiences of victims of financial identity theft in the Netherlands is less mature than in the United States which makes it more challenging to demonstrate the need for additional criminal legislation in light of victim assistance. Nevertheless, the limited information which is available indicates problems encountered by

---

[253] *Ibid.*

[254] Commission on Crime Prevention and Criminal Justice (2009). Thematic discussion: Economic fraud and identity-related crime. Eightteenth session, Vienna, 14 april 2009.

[255] Council of the European Union (2009). NOTE. Available at: http://eutrio.es/export/sites/trio/comun/descarga/PROGRAMA_TRxO_EN.pdf (last accessed July 12, 2010).

[256] *Stb.* 2009, 245.

[257] Director Instrumentation Procedures and Maintenance of Law and Order (2010).

victims when they attempt to resolve their problems through approaching law enforcement agencies. Maarten Kunst and Jan van Dijk examined the impact of financial-economic crimes on various types of victims of fraud, including victims of identity theft.[258] Based on a focus group, Kunst and van Dijk concluded how the victims involved in the study felt as though they had nowhere to go with their stories. All victims described how they received the sense that the relevant authorities suffered from a lack of knowledge about the topic of identity theft. One victim in particular described the process in detail about his attempt to report the problem at his local police station. The law enforcement officer at the station looked at him and stated: "You cannot file a report. You are not a victim. The credit card company is the victim."[259] The man pleaded with the officer and explained how he needed the report in order to prove his innocence to the credit card company. "She became infuriated," he told Kunst, "you don't even want to know how angry she became. But I told her, I am not leaving without a report."[260] Due to the victim's persistence, he finally obtained the police report, but his story provides an indication of the difficulty victims may face when they attempt to approach law enforcement officials in an effort to resolve the problem of identity theft.

The experiences of other victims also demonstrate the challenges faced by victims of identity theft, whether criminal or financial. The introduction of chapter 1 reflected on the heartbreaking story of Ron Kowsoleea and how the response provided to him by law enforcement proved particularly negative.[261] Whether the criminalization of identity theft can provide assistance to victims of the 'crime' is not supported by everyone. When asked whether she supported criminalization, the legal representative of Kowsoleea responded, "to answer that question, I need to think would that have helped my client and the answer is no. Because everything the perpetrator did is already criminalized. And criminalization of identity theft once again places the focus on the offender rather than the victim."[262]

3.2 Criminal Law Enforcement

3.2.1 United States

The role of the state as protector in the criminal realm extends beyond the mere introduction of substantive legislation to combat financial identity theft. Such legislation also needs to find its value in a world outside of Capitol Hill, primarily through its implementation by the law enforcement community. Enforcement of identity theft legislation presents a variety of challenges, especially as acts of identity theft occur in cyberspace. Those most often confronted by victims of the crime, State and local law enforcement officials, repeatedly acknowledge these challenges. Moreover, local and State law enforcement stress how "…the nature

---

[258] Kunst, M. J. J. & J. J. M. van Dijk (2009). *Slachtofferschap van Fraude: Een explorerend onderzoek na de impact van diverse vormen van financieel-economische criminaliteit*. International Victimology Institute Tilburg (INTERVICT).

[259] Audio recording of focus group held by Maarten Kunst (2010).

[260] *Ibid.*

[261] For other examples of identity theft victims in the Netherlands, see: De Nationale Ombudsman (2009). *De burger in de ketens*. Verslag van de Nationale ombudsman over 2008.

[262] Interview *de Vos & Partners Advocaten*, December 8, 2009, Amsterdam.

of identity theft investigations is generally beyond the technical capability and jurisdictional authority"[263] of lower level departments. Federal involvement is a requirement for identity theft cases, which federal agencies recognize. Various Federal agencies concern themselves with identity theft investigations, including the Department of Justice, the United States Secret Service, the Federal Bureau of Investigations, and the United States Postal Service.

In March 2010, the United States Department of Justice Office of the Inspector General published an audit report on the Department's efforts to combat identity theft.[264] The Deputy Assistant Attorney General demonstrated his awareness of the prevalence of identity theft and its status as the fastest growing crime in the United States during a congressional hearing.[265] Nevertheless, the Department of Justice does not maintain an internal identity theft strategy nor does the Department hold a person or entity with the responsibility of coordinating the identity theft efforts within the Department. More specifically the report states, "...the DOJ's approach to addressing identity theft has not been coordinated, resulting in identity theft not being treated as a DOJ priority."[266] The audit report also provides statistical data on the efforts made by the 94 United States Attorneys' Offices, who serve as the principal litigators and hold the responsibility of prosecuting federal criminal cases. The accumulation of statistical data on the number of identity theft cases charged and convicted is a result of a change in the case management of the Executive Office for United States Attorneys (EOUSA) which allowed Federal prosecutors to track identity theft cases via a specific subsection. This change occurred in December 2006 and the available data might therefore suffer from the time needed to adjust. As the report states, "...EOUSA officials stated that many USAOs were slow to adapt to this change and that, as a result, the more specific reporting category for identity theft likely understates the number of identity theft cases for FYs 2007 to 2009 because some such cases were likely reported under the broader offense code."[267]

Table 3.1
Identity Theft Defendants Charged and Convictions Obtained

	Identity Theft		Aggravated Identity Theft		Totals	
FY	Defendants charged	Convictions obtained	Defendants charged	Convictions obtained	Defendants charged	Convictions obtained
2007	269	103	532	272	744	365
2008	296	144	620	338	882	467
2009	239	138	578	296	769	432

The table above demonstrates the number of defendants charged in both categories of identity theft, along with convictions obtained. The available data

[263] Office of the Inspector General (2005). *Chapter 4: Summary of the Impact on the Law Enforcement Community.* Available at:
http://www.justice.gov/oig/reports/FBI/a0537/chapter4.htm (last accessed July 4, 2010).
[264] Office of the Inspector General (2010). *The Department of Justice's Efforts to Combat Identity Theft.* Audit Report 10-21.
[265] *Ibid.*
[266] *Ibid:* 4.
[267] *Ibid:* 9.

appears to depict a state of relative stability with respect to defendants charged and convicted. The information collection also appears a bit premature to draw reliable conclusions on the meaning of the number of defendant charges and convictions. In comparison to the statistics available on victims of identity theft, the totals do seem to reflect the complexity involved in the actual enforcement of the law due to the challenges invoked by the crime.

Perhaps the most important conclusion offered by the audit report is the lack of priority granted to the topic of identity theft by the Department of Justice. The issue of priority within an agency also deserves attention with respect to the Federal Bureau of Investigations (FBI), especially since its priorities experienced a crucial transformation after the events of September 11, 2001. The events of September 11, 2001 became widely viewed as a systemic intelligence failure of the United States Intelligence Community. This intelligence failure required organizational changes in the various components of the community, including the FBI. As the largest investigative agency, the FBI is responsible for the enforcement of more than 200 federal laws.[268] Before September 11, the FBI combined its national security responsibilities with other concerns such as criminal conspiracy, as its top priority. After the attacks, Robert Mueller III, Director of the FBI, initiated various changes including a reprioritization process.[269] Several months later, in May 2002, the FBI published its new list of priorities. Counterterrorism and counterintelligence topped the list. The FBI needed to be more equipped to combat imminent terrorist threats and to prevent other terrorist attacks against the United States. To accomplish its new counterterrorism objective, the FBI Director formally transferred more than 500 field agents from traditional crime areas to terrorism-related programs. The Director primarily transferred these resources from the FBI's Criminal Investigative Division (CID), which addresses traditional criminal areas such as narcotics trafficking and white-collar crime.

The third priority of the FBI became the protection of the United States against cyber-based attacks and high-technology crimes. A *distant* third priority, according to Brian Krebs.[270] For a third place on the priority list, cybercrime receives relatively few resources. In its Fiscal Year 2008 Budget Request, the Justice Department demanded $258.5 million in funding and approximately 659 field agents for the 'third priority.' Out of a total of 11,868 FBI agents nationwide, 659 comes down to approximately 5.5 per cent. A closer look, however, provides even more important indicators about the dedication of agents and funds. The 'Innocent Images National Initiative' receives the involvement of nearly one third of the agency's cyber agents. This program is a child pornography initiative which aims to catch those who look at or facilitate the production of such pornography. Despite the importance of such a program, the remaining resources for other types of cybercrime paint a dismal picture. Less than 4 per cent of all field agents dedicate their time to the fight against other types of cybercrime. Whether this is a direct result of the focus on terrorism is difficult to determine.

---

[268] Masse, T. & W. Krouse (2003). *The FBI: Past, Present, and Future.* CRS Report for Congress.
[269] Office of the Inspector General. (2004). *The Internal Effects of the Federal Bureau of Investigation's Reprioritization.* Audit Report 04-39.
[270] Krebs, B. (2007). Is Cyber Crime Really the FBI's No. 3 Priority? Available at: http://voices.washingtonpost.com/securityfix/2007/09/is_cyber_crime_a_distant_3rd_p.html (last accessed July 4, 2010).

After the implementation of the reprioritization process, the Office of the Inspector General (OIG) conducted audits to examine the effects, both internal and external, of the changes. The decrease in financial crime cases dealt with by the FBI is drastic. The FBI handled 17,402 cases in 2000 in comparison to 10,463 in 2004.[271] Other crimes, namely violent crimes, also demonstrate a substantial decrease in the number of cases. Identity theft data is less readily available due to the lack of registration prior to 2003. Yet, as the OIG notes, "…identity theft is often part of larger fraud schemes and the FBI may have been involved in many more identity theft investigations through cases tracked under different investigative classifications."[272] In general, the actual influence of the organizational changes introduced after the events of September 11 remain difficult to establish. The Government Accountability Office (GAO) reported in 2004 how the data proved inconclusive with respect to the effects of the reprioritization on the efforts to combat drug, white-collar, and violent crime.[273]

The OIG Audit Report in 2005, on the other hand, concluded how there was a significant reduction in the FBI's investigative efforts with regard to fraudulent activities involving financial institutions.[274] In particular, lower dollar cases suffered as a result of the reduction. A similar investigative gap exists for telemarketing and wire fraud. Prior to its official registration, identity theft cases most likely found themselves included in any of the various categories described above, such as financial or white-collar crime.

Despite the dispute about the actual priority granted to criminal areas outside of the national security realm, the FBI managed several moments of success with regard to identity theft cases. Since 2003, when official registration began, the FBI has been involved in thousands of identity theft cases. Of the 1255 pending cases in 2006, the FBI managed to secure 457 indictments and 405 convictions of perpetrators of identity theft. Furthermore, the FBI also obtained $156.5 million in Restitutions, $4.3 million in Recoveries, and $1.2 million in Fines.[275] The previously cited audit report of March 2010 describes a more positive reflection of the prioritization process within the FBI with respect to identity theft. As the report notes, ""[a]lthough the specific crime of identity theft is not a top FBI priority, the FBI frequently addresses identity theft through the Cyber Division's criminal intrusion program, which is currently a top FBI priority. According to a senior FBI official, the FBI determined that it must prioritize the use of its resources, and he believed that the FBI would have the greatest impact on identity theft by primarily addressing the crime through its Cyber Division."[276] Not everyone within the agency agreed with this approach.[277]

Unfortunately, the FBI no longer collects statistical information on investigations and convictions related to identity theft which makes it difficult if not impossible to assess its impact and the actual priority granted to the problem

---

[271] Office of the Inspector General (2005). *The External Effects of the Federal Bureau of Investigation's Reprioritization Efforts*. Audit report 05-37.
[272] *Ibid*, Chapter 9 Identity Theft.
[273] Government Accountability Office (GAO) (2004a). *FBI Transformation: Data Inconclusive on Effects of Shift to Counterterrorism-Related Priorities on Traditional Crime Enforcement*, Report Number GAO-04-1036.
[274] Office of the Inspector General (2005).
[275] Federal Bureau of Investigations (2006). *Financial Crimes Report to the Public Fiscal Year 2006*.
[276] Office of the Inspector General (2010): vi.
[277] The audit report states, ""[t]wo supervisory-level FBI employees with substantial knowledge about identity theft told us that they did not agree with the decision to transfer control of the FBI's identity theft program to the Cyber Division."

by the agency. The audit division of DOJ underscores this complexity and expresses its concerns when it writes, "[w]e are concerned about the FBI's lack of identity theft data and mandatory comprehensive assessments on the threat of identity theft. Without such data and comprehensive assessments the FBI cannot maintain a current understanding of the threat presented by identity theft or properly coordinate its approach to a crime that cuts across multiple FBI program areas, including counterterrorism, and victimizes millions of Americans each year."[278] Nevertheless, the Cyber Division managed to conduct its own assessment through examining the 1,180 pending computer intrusion investigations between FYs 2007 and 2009. Through its examination, the division concluded how 62 per cent of the pending cases mentioned above concerned the crime of identity theft.[279]

The FBI rarely operates alone. As previously noted, the Secret Service also holds an important position in the enforcement of identity theft legislation. Officially, under 18, U.S.C. Section 1028, the Secret Service is the primary Federal agency tasked with the investigations of identity theft cases. In FY 2008, the Secret Service arrested over 5,600 suspects of crimes related to identity theft.[280] The Secret Service maintains 35 Financial Crime Task Forces and 24 Electronic Crime Task Forces that investigate identity theft cases, along with various other crimes. Since July 2009, there are three new Electronic Crime Task Forces. In the press release announcing the additional Task Forces, Secret Service Director Mark Sullivan proclaimed "[o]ne of the top priorities for the Secret Service continues to be combating the computer related crimes perpetrated by domestic and international criminals that target the U.S. financial infrastructure."[281] Sullivan's statement coincides with the United States Secret Service Strategic Plan (FY 2008-2013), which lists protecting the nation's financial infrastructure by reducing losses due to counterfeit currency, financial and electronic crimes and identity theft as its primary strategic goal.[282]

Besides the FBI and the Secret Service, the United States Postal Inspection Service also plays a role in identity theft investigations, especially when perpetrators used the postal service to commit their crime. The last update on the number of arrests made by the United States Postal Inspection Service with respect to identity theft came in 2007. During that year, the Postal Service reported 2,071 identity theft arrests.[283]

3.2.2 The Netherlands

Enforcement of identity theft cases is difficult to assess due to the lack of a separate criminal offense in the Netherlands. This section shall therefore review the treatment of identity theft in policy documents of the law enforcement

---

[278] *Ibid:* vii.

[279] *Ibid:* 20.

[280] Finklea, K. M. (2009). *Identity Theft: Trends and Issues*. Congressional Research Service.

[281] United States Secret Service (2009). U.S. Secret Service Forms Three New Task Forces: Electronic crimes partnerships bring together law enforcement, academia and private sector. Press Release, July 10, 2009. Available at: http://www.secretservice.gov/press/GPA06-09_NewECTFs.pdf (last accessed July 4, 2010).

[282] United States Secret Service (n.d.). *United States Secret Service Strategic Plan*. Available at: http://www.secretservice.gov/usss_strategic_plan_2008_2013.pdf (last accessed July 4, 2010).

[283] United States Postal Investigation Services (2007). *Annual Report of Investigations of the United States Postal Services*.

community and also describe activities in other related areas of crime, such as cybercrime and financial-economic criminality. The discussion of law enforcement priorities provides a valuable indication of the importance granted to identity theft in the community. The Ministry of the Interior published the National Police Services Agency Priorities for 2008-2011 in 2007.[284] These priorities reflect the government's goals with regard to crime in society. Its main goal is to decrease crime by 25% in 2010 in comparison to the percentage of crime in 2002. To achieve its goal, the government demands a dominant focus on violent crimes, the development of safe neighborhoods, juvenile delinquency and youth at risk. In contrast to the previously mentioned priorities, the last priority, which is to improve both the quality of investigations and the quantity, discusses certain relevant areas. The policy document mentions cybercrime along with organized and financial crimes. Identity theft displays characteristics which fit in all of these categories; yet, identity theft is never specifically mentioned during the description of the above types of crime. Instead, in the category cybercrime child pornography explicitly receives the highest priority for the national police.[285] For organized crime, the primary focus appears to be on human trafficking, prostitution, money laundering and illegal drug production and trade. The description of financial crimes refers to fraud, but fails to specifically identify identity theft as a priority in that category. The focus herein is on national priorities and therefore excludes potential variations on local levels of the law enforcement community. Important to note still is how certain local departments are in pilot programs which intensify the fight against financial economic crimes. This intensification which is referred to as 'program financial economic crimes' is the result of the government's aim to visibly reduce organized crime by the end of 2011.

Moreover, the government specifically wants to prevent the threatening link between the underground world and the legal or 'upper world.'[286] The government announced its plan at the end of 2007 and specifically identified human trafficking, the infiltration of illegal activities in the real estate sector, and the grand production of soft drugs as focus areas of the program. The intensification of the investigation of financial economic criminality and the reduction of criminal money are also aspects of this umbrella plan. For financial economic crimes, the government mentions money laundering, fraud, and corruption. In order to establish an effective fight against organized crime, the government emphasizes the need for cooperation among the various parties involved in the area of crime prevention and repression. The government recognizes how financial economic criminality is an umbrella term but all of the crimes which fall within the category maintain a dominant financial and business aspect. In the policy plan, the government refers to identity theft briefly in the description of fraud in general.[287]

The results of the overarching program which focuses on security through prevention provide a promising outlook, according to the government. For the area of serious and organized crime, the focus is on the reduction of opportunity structures in an effort to produce obstacles for the occurrence of such crimes.

---

[284] Korps Landelijke Politiediensten (KLPD) (2007). *Prioriteiten KLPD 2008-2011*.
[285] *Ibid.*
[286] Ministerie van Justitie (2007). Kabinet: 'bestrijding georganiseerde misdaad versterken.' *Press Release*, December 13, 2007.
[287] See *Kamerstukken II* 2007 – 2008, 29911, nr. 10: 2.

Main examples include the successful investigation of real estate fraud and human trafficking, along with large soft drug production operations.[288]

More relevant is the intensified cooperative effort between law enforcement and the public prosecutor's office in the fight against fraud. This cooperation also includes the private sector, such as the Dutch Banking Association especially with regard to credit card fraud. Together these parties aim to establish societal barriers to complicate the efforts of perpetrators to commit various crimes, including account takeover of credit cards.[289]

Despite the lack of direct attention granted to identity theft in the most recent list of police priorities discussed above, other sources do mention identity theft. A headline in 2008 described an intensified approach to identity theft by the Dutch police. Wim van Vemde, police superintendent, issued a warning for the potential spread of 'American experiences.' Van Vembe recognizes how the United States certainly faces more significant numbers and more severe cases of identity theft, but he acknowledges how experience teaches the Netherlands that whatever happens in the United States ultimately comes our way.[290]

Positive news about investigations and reduction of criminal operations related to identity theft provide a representation of this intensified approach. Several years ago, in 2007, the Team High Tech Crime (THTC) began its operations as part of the National Police Services Agency (KLPD). After only one month, a Dutch bank arrived at the doorstep of the THTC with a case. Through a sophisticated phishing scam, perpetrators managed to successfully carry out a Man in the Middle Attack[291] and drain accounts of 200 clients. The bank involved asked the THTC team to investigate the case.[292] The investigation led to Hong Kong, but traces of those behind the operation died soon upon arrival. The THTC managed to proceed with the investigation after the incorporation of a particularly innovative method. A colleague within the team received a money mule recruitment email. Money mules, as shall become more obvious in chapter 7, function as a transfer channel for criminal proceeds in an effort to divert and confuse the audit trail. Basically, money mules receive the money from the victim's account and transfer it to an offshore account. For their effort, mules generally receive a small percentage of the money. The THTC responded to the recruitment email and as a result received the money taken from the accounts of the victims.

During the following years, the THTC used previous experiences to expand its capacity and knowledge about identity theft operations. Whereas the first year predominantly dictated a case based approach which meant the team reacted to events rather than initiating proactive measures to reduce crime, the latter years demonstrate progress. From case to phenomenon based, the THTC aims to

---

[288] Ministerie van Justitie (2010). *Verantwoording veiligheid begint bij voorkomen.*

[289] From various corners, however, financial service providers, from credit card companies to banks, have infomrally and off the record expressed how law enforcement does not consider the investigation of financial identity theft cases a priority.

[290] Politie opent offensief tegen identiteitsfraude. *Trouw*, August 7, 2008. Available at: http://www.trouw.nl/nieuws/laatstenieuws/article1737530.ece/Politie_opent_offensief_tegen_identiteitsfraude.html (last accessed July 12, 2010).

[291] The Man in the Middle or Man in the Browser attack receives more extensive coverage in chapter 5, but succinctly the attack refers to an incident where perpetrators manage to place themselves between the client and the financial service provider. As a result, the perpetrator intercepts the communication and captures the necessary information in an effort to carry out or otherwise redirect transactions.

[292] Interview Team High Tech Crime, December 6, 2007, Driebergen.

anticipate innovative means used by perpetrators to commit identity theft.[293] THTC specifically targets the top of the criminal pyramid, which represent the innovators of methods used to carry out their criminal activities.[294]

Other initiatives also target identity theft operations through an overarching approach to cybercrime. The public prosecutor's office mentions identity theft during its discussion of cybercrime in its 'perspective on 2010' which the office published the previous year. The public prosecutor's office acknowledges how the increased use of information-and communication technology develops a more significant opportunity structure for crime to occur. The office mentions identity theft as an example of a crime which can occur as a result of such an opportunity structure.[295] Further along, the public prosecutor's office returns to identity theft and identifies the problem as part of the 'new themes' which the office shall encounter during the upcoming years.

The public prosecutor's office together with law enforcement commenced a program which specifically focused on an intensified approach to cybercrime. As part of this program, both parties introduced 'experimental gardens.' These gardens focus on specific areas of cybercrime such as child pornography, fraud on the Internet, and ICT as a target of crime. Within these experimental gardens, various organizations, including the public prosecutor's office, law enforcement, municipalities, and private parties, work together and 'experiment' through the usage of new investigation methods which they apply to genuine criminal cases. The focus of the gardens extends beyond the mere prosecution of suspects in a single case, instead the cooperative effort also aims to develop an understanding of the underlying structures which facilitate and subsequently maintain the existence of such criminality. This is why gardens work with a 'barriermodel.'[296]

The interesting aspect of the criminal law enforcement approach presented in the Netherlands with respect to cybercrime in general is the incorporation of the situational crime prevention framework. This becomes apparent since much of the discussion of the initiatives demonstrates the focus on opportunity reduction. As a result, criminal law enforcement surpasses the more traditional approach of crime fighting through 'catching the criminal' and also implements means to potentially alter the opportunity structure of financial identity theft.

3.2.3 Transnational Enforcement

As noted in the overview above, identity theft and cybercrime demonstrate a significant connection in contemporary society. Such a connection means the challenges law enforcement units face with respect to cybercrime are also applicable to financial identity theft. In particular the transnational challenges which complicate the efforts made by law enforcement professionals. The investigation of identity theft cases which incorporate digital technology require particular expertise along with considerable time and resources. The international aspect of the problem in particular complicates the investigation and subsequent prosecution of cases. To mitigate these challenges and complicating factors, the

---

[293] Hunting cyber criminals: the next level (2009). Presentation given at the GOVCERT.NL Symposium, October 7, 2009, Rotterdam, the Netherlands.
[294] Expert Meeting Cybercrime April 13, 2010, Maarsen, the Netherlands.
[295] Openbaar Ministerie (2006). *Perspectief op 2010*.
[296] 'Intensiverings programma's Openbaar Ministerie.' See http://www.om.nl/cybermap/expertmeeting/wat_is_het_pac/ (last accessed July 14, 2010).

Council of Europe introduced several initiatives in the fight against cybercrime. After two non-binding recommendations – about substantive criminal law in 1989 and procedural criminal law in 1995 – turned out to have insufficient impact on national legislation, the Council took the initiative for a binding legal instrument, which led to the Convention on Cybercrime of 2001.[297]

The Council of Europe Convention on Cybercrime has three principal aims.[298] The first aim is to harmonize domestic criminal substantive law elements of offenses and related provisions in the area of cybercrime. The second aim is to provide for domestic criminal procedural law powers necessary for the investigation and the subsequent prosecution of such offenses as well as related offenses. The third aim is to establish a fast and effective regime of international cooperation. The Convention classifies the offenses into five areas of substantive criminal law including computer-related offenses such as computer-related forgery and computer-related fraud, but also offenses against the confidentiality, integrity and availability of computer data and systems, which include illegal access, interception, data and system interference, and misuse of devices.[299] Other, for identity theft less relevant, offenses include child pornography and offenses related to the infringement of copyright and related rights. The Convention calls for the adoption of legislative and other measures where necessary in order to establish the above mentioned offenses as criminal offenses under domestic law. This call is a response to the need for criminal law to "...keep abreast of these technological developments which offer highly sophisticated opportunities for misusing facilities of the cyber-space and causing damage to legitimate interests. Given the cross-border nature of information networks, a concerted international effort is needed to deal with such misuse."[300]

The collection of evidence is a particularly complex issue for cybercrime in general and identity theft conducted via the Internet in particular. This is because of forensic problems which accompany the collection of 'digital evidence.' As the United Nations notes in its background paper on measures to combat computer-related crime, "[p]art of the problem in reconstructing an incident involving a cybercrime is that much of the evidence is intangible and transient. Rather than physical evidence, cybercrime investigations seek out digital traces that are often volatile and short-lived."[301] Moreover, digital traces usually provide evidence of a link between the offense and a computer or IP address, but not necessarily a link between the offense and a person behind the computer. Identifying individual perpetrators is one of the major challenges for digital investigations. Closely related to the difficulty of actually capturing the digital evidence is the need for particular resources and expertise. As Deputy Assistant Attorney General Malcolm notes, "[w]e are clearly no longer in an age where law enforcement agents can defeat criminals with a badge, a flashlight, and a gun."[302] All of these complexities

---

[297] Kaspersen, R. (2007). 'Het Cybercrime-verdrag van de Raad van Europa,' in E. J. Koops (ed.) *Strafrecht & ICT*. Den Haag: SDU Uitgevers : 137 – 180.
[298] Council of Europe (2001). Explanatory Report to the Council of Europe Cybercrime Convention.
[299] See Council of Europe Cybercrime Convention Title 2 – Computer-related offences.
[300] Council of Europe (2001). Explanatory Report to the Council of Europe Cybercrime Convention, paragraph 9.
[301] United Nations (2005). Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Workshop 6: Measures to combat computer-related crime: Background paper: 11.
[302] Malcolm (2003). Remarks before the OECD-APEC Global Forum. Available at: http://www.justice.gov/criminal/cybercrime/JGM_OECD.htm (last accessed July 12, 2010).

are magnified due to the cross-jurisdictional nature of cybercrime in general, and financial identity theft in particular.

The Convention therefore provides 'instruments' or at least intends to do so in an effort to stimulate cooperation. Article 35 of the Convention establishes the 24/7 network which requires each party to designate a point of contact which is available on a twenty-four hour basis for seven days a week. Such a network is designed to ensure immediate assistance for investigations or proceedings with regard to criminal offenses related to computer systems and data, or for such assistance in connection to the collection of evidence of a criminal offense, in electronic form. The Convention specifies the type of assistance to include the facilitation of technical advice and the preservation of data pursuant to Articles 29 and 30.

Furthermore, the 24/7 network can also provide assistance with the collection of evidence and through providing legal information, and through locating suspects. Due to the volatile nature of digital evidence along with the challenges associated with the investigation of cross-border crimes, the network is an essential feature of the overall transnational approach to cybercrime. The drafters of the Convention therefore considered the network to be one of the most important means for an effective response to the challenges encountered by law enforcement as a result of cybercrime. Moreover, the drafters based their decision for the network on the demonstrated effectiveness of a previously functioning network.[303]

The Convention also requires parties to adopt legislation which facilitates the investigation of cybercrime cases. Such facilitation is intended to occur through the expedition, preservation, and production of electronic evidence.[304] Other means of investigation facilitation can occur through the application of search and seizure law to data stored on computer systems, the authorization for law enforcement agencies for real-time collection of traffic data, and the interception of content data.[305]

The provisions set forth in the Convention provide valuable assistance, especially through the 24/7 network and investigative powers for mutual assistance, but challenges remain. These challenges partly occur due to the existence of data havens. As Jeremy N. Geltzer writes, "[a] data haven provides a safe harbor beyond the reach of any government's jurisdiction, and offers its users maximum security and minimal regulation."[306] Important countries with respect to cybercrime such as Russia and China have not signed or ratified the Convention. This demonstrates the limited applicability of the Convention to those countries who have demonstrated their commitment to the problem through their ratification.[307] Susan W. Brenner notes how the pace of ratification is surprisingly low which complicates the assessment of its impact for the fight against cybercrime. As Brenner states, "[t]he prime movers behind the Convention have ignored it for three years; ratification and implementation are obviously not a high priority for these countries. Their inaction is puzzling and somewhat unsettling. It

---

[303] Council of Europe (2001). Explanatory Report to the Council of Europe Cybercrime Convention.
[304] Articles 16 – 18.
[305] Articles 19 – 21.
[306] Geltzer, J. N. (2003). The New Pirates of the Caribbean: How Data Havens Can Provide Safe Harbors on the Internet Beyond Governmental Reach. *Southwestern Journal of Law & Trade in Americas*, Vol. 10: 435.
[307] As of June 21, 2010, 30 countries ratified the Cybercrime Convention.

may be, as the conference speaker suggested, that the Convention is falling prey to its own ambitions—that the nature and extent of the effort required to implement it is discouraging countries from ratifying it."[308] The success of the Convention rests on the ratification of the document by countries around the world. For such ratification is imperative, as Brenner notes, otherwise the 'haven' scenario remains unaddressed.[309]

3.3 Data Protection Legislation

In *The Digital Person*, Daniel J. Solove describes how "[t]he underlying cause of identity theft is an architecture that makes us vulnerable to such crimes and unable to adequately repair the damage. This architecture is not created by identity thieves; rather, it is exploited by them. It is an architecture of vulnerability, one where personal information is not protected with adequate security, where identity thieves have easy access to data and the ability to use it in detrimental ways."[310] Solove emphasizes and demonstrates the importance of data protection, or the lack thereof, in light of the facilitation of identity theft. Through his description of the architecture of vulnerability, he reveals how the treatment of personal information by both the public and the private sector merit attention due to their connection with the facilitation of identity theft. Perpetrators of identity theft need personal information of potential victims to carry out their activities en route to financial profits. Such information is often maintained by various organizations in both the public and the private sector and therefore attractive for perpetrators. The access to such information is largely dependent on the protection offered by the state through its role as protector. As the Identity Theft Task Force acknowledged in its strategic plan, "[i]dentity theft depends on access to consumer data. Reducing the opportunities for thieves to get the data is critical to fighting the crime. Government, the business community, and consumers have roles to play in protecting data."[311]

3.3.1 United States

The concept of privacy is far more commonly used than the notion of data protection in the United States. Every day speech along with relevant legislation refers to privacy rather than data protection. Privacy in a broad sense, however, also encompasses informational privacy, which is the functional equivalent of data protection. The common perception credits the legal origin of privacy, or rather the right to privacy, to its 'founding fathers' Samuel Warren and Louis Dembitz Brandeis. More than a century ago, in 1890, Warren and Brandeis published 'The Right to Privacy' in *Harvard Law Review*. The piece continues to receive much admiration for its landmark contribution to the privacy debate. Benjamin E. Bratman, for example, notes how "[i]n the more than 110 years since its publication, Brandeis and Warren's article has attained what some might call

---

[308] Brenner, S. W. (2007). 'The Council of Europe's Convention on Cybercrime,' in J. M. Balkin, J. Grimmelmann, E. Katz, N. Kozlovski, S. Wagman & T. Zarsky (eds.) *Cybercrime: Digital Cops in a Networked Environment*. New York: New York University Press: 217.
[309] *Ibid.*
[310] Solove, D. J. (2004). *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press: 115.
[311] Identity Theft Task Force (2008). *The President's Identity Theft Task Force Report*: 4.

legendary status. It has been widely recognized by scholars and judges, past and present, as *the* seminal force in the development of a 'right to privacy' in American law."[312]

Warren and Brandeis commence their plea through the description of the actions of journalists, especially photojournalists, who were, according to the authors, overstepping the apparent boundaries of propriety and decency. More specifically, the authors indicate how "[r]ecent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual...the right 'to be let alone.'"[313] This 'next step' represents a logical continuance in the expansion of the scope of legal rights of individuals to have full protection in person and in property. Warren and Brandeis trace the evolution of these legal rights in order to determine "...whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is."[314] To demonstrate how existing law affords such a principle, Warren and Brandeis draw analogies to the law of slander and of libel, the law of (intellectual) property and the law of trade secrets. Robert Ellis Smith describes how the analogies drawn by Warren and Brandeis allowed them to develop the right to privacy. Smith summarizes: "[i]f the common law of slander and of libel provide damages for injury to one's reputation, why not a remedy for damage to one's feelings even if what was said or published is true? If one can control publication of one's intellectual property through copyright and other restrictions in the law, why not a right to control publication of one's other intimacies? If organizations can protect trade secrets, why can't individuals protect personal secrets?...If the law of other countries recognizes the right to privacy, why not the United States?"[315]

The persuasive power of Warren and Brandeis altered the privacy landscape in the United States. Nevertheless, Alan F. Westin provides a different sound and states "...the notion put forward by legal commentators from Brandeis down to the present—that privacy was somehow a 'modern' legal right which began to take form only in the late nineteenth century—is simply bad history and bad law. Pre-Civil War America had a thorough and effective set of rules with which to protect individual and group privacy from the means of compulsory disclosure and physical surveillance known in that era."[316] At the same time, Westin clearly states how "[t]his discussion is not intended to minimize the value of the Warren-Brandeis approach between 1890 and 1950 as a path-breaking contribution to modern conceptions of privacy as a legal right of the individual."[317] Westin especially notes how the 'common-law movement' led by Warren and Brandeis assisted in the analysis of the importance of privacy in American society, the proper claims of personal privacy, and the assessment of the importance of the right to privacy in competition with other social interests. Through this contribution, Warren and Brandeis assisted in the establishment of legal sensitivity

---

[312] Bratman, B. E. (2002). Brandeis and Warren's *The Right to Privacy* and the Birth of the Right to Privacy. *Tennessee Law Review*, Vol. 69: 624.
[313] Warren, S. & L. D. Brandeis (1890). The Right to Privacy. *Harvard Law Review*, Vol. 4 (5): 195.
[314] *Ibid:* 197.
[315] Smith, R. E. (1993) *The Law of Privacy Explained.* Providence, RI: Privacy Journal: 7.
[316] Westin, A. F. (1973) *Privacy and Freedom.* New York: Atheneum: 337 – 338.
[317] *Ibid:* 349.

to privacy as an independent interest, rather than a dependent adjunct of property or liberty.

Warren and Brandeis influential work is most valuable in privacy-related discussions; yet, on a more abstract level, their line of legal reasoning also illustrates the need for government officials, whether policy makers or those in the judiciary branch, to accept and subsequently promote the inherent fluidity of law. Such fluidity is crucial in light of changes and additional demands introduced into society, which lead to novel challenges. This became particularly evident during the second half of the twentieth century. During that era, the introduction of and subsequent use of the computer along with its increased storage capacity presented a new privacy chapter with its accompanying challenges. In 1965, the House of Representatives Committee on Government Operations created a special subcommittee to investigate the invasion of privacy.[318] The special subcommittee held a variety of hearings throughout the following years.[319] In a similar vein, the Senate Committee on the Judiciary activated its Subcommittee on Administrative Practice and Procedure to hold numerous hearings on the Invasion of Privacy. From hearings about the more general invasion of privacy, the various subcommittees began more specific investigations into the role of the computer in relation to privacy and the potential for invasions.[320]

Around the same time, Westin published his *Privacy and Freedom*, which, according to James B. Rule *et al.*, "…shaped virtually all current thinking about privacy as a public issue."[321] Westin describes how privacy's rise to the top of the political agenda is a result of political officials "[r]eaching to each other from opposite ends of the American political spectrum, conservatives and liberals united in alarmed reaction at 'computerized Big Brother.'"[322] Whereas he credits the common-law movement initiated by Warren and Brandeis, he also recognizes how "[t]he seed was there, but in this era the warmth of public support to nurture it was lacking."[323] The importance of Westin's contribution rests in his eloquent description of privacy and its place in the United States, both in the past as well as in the present. In his final chapter, he describes "[t]he explorations of surveillance technology and techniques, public reactions to these pressures, the functions that privacy serves for individuals and society, and the concept of privacy in American law—all these have been attempts to acquire a firm understanding of privacy in contemporary America. With such a basic understanding, the hard problems of balance and choice can be met; without such knowledge, both the public and the legal specialists might be tempted to seek simplistic formulas which will neither control intrusive technology nor set a proper balance of privacy."[324] Through the understanding set forth by Westin, he develops criteria which assist weighing conflicting interests. The development of these criteria allows privacy to receive its proper weight when conflicting interests require the establishment of a balance.

In addition to Westin's groundbreaking contribution and the many Congressional hearings came a report 'Records, Computers, and the Rights of

---

[318] Regan, P. M. (1995). *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill, NC: University of North Carolina Press.
[319] *Ibid.*
[320] For an extensive overview of hearings held see *Ibid.*
[321] Rule, J. B., McAdam, D., Stearns, L. & D. Uglow (1980). *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies*. New York: Elsevier: 73.
[322] Westin (1973): 321.
[323] *Ibid:* 349.
[324] *Ibid:* 365.

Citizens.'[325] Due to the growing concern about the potential consequences resulting from the uncontrolled application of computer and telecommunications technology to collect, store, and use data about individual citizens, former Secretary of Health, Education, and Welfare (HEW), Elliot L. Richardson established 'the Secretary's Advisory Committee on Automated Personal Data Systems.'[326] The Advisory Committee received the task to analyze and make recommendations about "[h]armful consequences that may result from using automated personal data systems; Safeguards that might protect against potentially harmful consequences; Measures that might afford redress for any harmful consequences; Policy and practice relating to the issuance and use of Social Security numbers."[327] The Committee's insights with regard to the last task will receive considerable attention in section 4.2.1. With respect to the other tasks the Advisory Committee concludes, "[u]nder current law, a person's privacy is poorly protected against arbitrary or abusive record-keeping practices. For this reason, as well as due to the need to establish standards of record-keeping practice appropriate to the computer age, the report recommends the enactment of a Federal 'Code of Fair Information Practice' for all automated personal data systems."[328] This Code is based on the following five principles:

- ✓ There must be no personal data record keeping systems whose very existence is secret.
- ✓ There must be a way for an individual to find out what information about him is in a record and how it is used.
- ✓ There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
- ✓ There must be a way for an individual to correct or amend a record of identifiable information about him.
- ✓ Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

Particularly due to its uncanny ability to illustrate the dangers along with the most promising safeguards, the HEW Report maintains an important place in the history of information privacy in the United States. The HEW Report alone, however, may never have generated as much attention if its publication had not occurred around the same time as a crucial political event. Rule describes how "[t]he Watergate drama, with its many twists and subplots, did perhaps more than anything else to force official treatment of personal data into the arena of public controversy."[329] Colin Bennett coincides with this perspective and also emphasizes how the Watergate crisis provided the necessary climate to open a policy window for the privacy issue. Bennet states, "[t]he many and various cases of political

---

[325] Health, Education, and Welfare Advisory Committee (1973). *Records, Computer, and the Rights of Citizen*. Report of the Secretary's Advisory Committee on Automated Personal Data Systems.
[326] *Ibid.*
[327] *Ibid.*
[328] *Ibid.*
[329] Rule, J. B. (1974). *Private Lives and Public Surveillance: Social Control in the Computer Age*. New York: Schocken Books: 62.

bribery, corruption, malpractice, intrusiveness, and abuse of personal data that are captured by the emotive term 'Watergate' gave the privacy advocates the perfect horror story."[330] Whereas the HEW Report described the potential harmful consequences, Watergate managed to provide the powerful illustration to 'back up the story.' The subsequent legislative action and especially the rate at which the legislation passed both the Senate and the House of Representatives became a direct result of the political momentum going on in Washington. The enactment of the Privacy Act of 1974 is, according to Bennett, "...part of a wider effort to open up the executive establishment and cleanse the government of the murky and conspirational influences of the Nixon White House."[331] Ironically, former President Richard Nixon, perhaps in an attempt to conduct necessary damage control, held a radio address on February 23, 1974, about the American right to privacy.[332] In his address, Nixon says:

> "At no time in the past has our Government known so much about so many of its individual citizens. This new knowledge brings with it an awesome potential for harm as well as good—and an equally awesome responsibility on those who have that knowledge. Though well-intentioned, Government bureaucracies seem to thrive on collecting additional information. That information is now stored in over 7,000 Government computers. Collection of new information will always be necessary. But there must also be reasonable limits on what is collected and how it is used."[333]

Further along, he acknowledges the harmful consequences, when he states:

> "In some instances, the information itself is inaccurate and has resulted in the withholding of credit or jobs from deserving individuals. In other cases, obsolete information has been used, such as arrest records which have not been updated to show that the charges made against an individual were subsequently dropped or the person found innocent. In many cases, the citizen is not even aware of what information is held on record, and if he wants to find out, he either has nowhere to turn or else he does not know where to turn."[334]

Nearly four decades later, Nixon's words still hold value. The situation he depicts contains frightening similarities with the consequences experienced by victims of financial identity theft. His radio address, coincidentally, was not the first time Nixon came to defend the right to privacy. As a private attorney in 1966, before his presidency, Nixon appeared in the United States Supreme Court. In *Time, Inc.* v. *Hill*, Nixon represented the Hill family against *Life* magazine. Based on his personal conviction and agreement with Warren and Brandeis, about the 'right to

---

330 Bennett, C. J. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithica, NY: Cornell University Press: 71.
331 *Ibid:* 72.
332 Nixon, R. (1974). Radio Address about the American Right of Privacy. Available at: http://www.presidency.ucsb.edu/ws/index.php?pid=4364 (last accessed July 12, 2010).
333 *Ibid.*
334 *Ibid.*

be let alone', Nixon decided to represent Hill.[335] Time, Inc. won the case in the end. And Nixon appeared devastated. His behavior in public, however, was in stark contrast with his actions behind the scenes. Rachel Brady describes how during the years in the White House, "...Nixon learned a great deal from the way Johnson treated personal privacy. Amongst other things, he adopted Johnson's use of the FBI and other investigatory agencies to further his political ends while publicly behaving like a crusader for personal privacy protection. To the public, still recoiling from Johnson and the FBI, Nixon was a champion of personal privacy protection."[336] Nevertheless, in an indirect way, Nixon's actions ultimately led to an increase in privacy legislation. As previously noted, the Privacy Act of 1974 passed rapidly after Watergate. The Act incorporates many of the recommendations made by the HEW Report. Its focus is exclusively on personal information maintained by the public sector. The Act is "...the only omnibus act that protects informational privacy." [337]

The Privacy Act of 1974[338] remains the most important piece of legislation with regard to information privacy for the public sector.[339] The Privacy Act states, among other things, how "[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains."[340] The Act makes several exceptions to this requirement.[341] Robert Gellman writes "[i]n some ways, the Privacy Act was a tremendously influential piece of legislation. It was the world's first attempt to apply the principles of fair information practices...This does not mean the Privacy Act was a success at home. There is a big difference between adopting good policies and implementing them well. A review of the act under the framework of fair information practices illustrates the statutory and administrative shortcomings."[342]

Additional legislation with regard to information privacy for the public sector is more specific and therefore maintains limited applicability. Main examples include the Family Educational Rights and Privacy Act (FERPA) of 1974 which establishes and regulates the conditions under which educational agencies may disclose information about their students to others with or without the prior consent of the individual[343], and the Health Insurance Portability and Accountability Act (HIPPA) of 1996, which regulates the protection of

---

[335] Brady, R. (2007). *From Court to Country: A Legal, Social and Political Analysis of Privacy in the U.S., 1965-1974*. Unpublished thesis. Available at: http://digitalcommons.macalester.edu/cgi/viewcontent.cgi?article=1004&context=poli_honors (last accessed July 12, 2010).

[336] *Ibid*: 73.

[337] Shaffer, G. (1999). The Power of EU Collective Action: The Impact of EU Data Privacy Regulation on US Business Practice. *European Law Journal*, Vol. 5 (4): 422.

[338] 5 U.S.C. § 552a

[339] Important and interesting to note is how the Privacy Protection Study Commission which published its report *Personal Privacy in an Information Society* in 1977 recommended an extension of the Privacy Act to include the private sector, and the regulation of Social Security Numbers, but the United States Congress ignored these recommendations.

[340] *Ibid.*

[341] See Conditions of Disclosure.

[342] Gellman, R. (2001). 'Does Privacy Law Work?' ' in P.E. Agre & M. Rotenberg (eds.) *Technology and Privacy: The New Landscape.* Cambridge, MA: MIT Press: 196.

[343] 20 U.S.C. § 1232g

individually identifiable health information in the health care sector and establishes penalties for wrongful disclosure of such information.[344]

In addition to data protection for educational and health records, the government also established the Driver's Privacy Protection Act of 1994[345] (DPPA) which prohibits the release or use of personal information by any State Department of Motor Vehicles (or any officer, employee, or contractor thereof) about an individual obtained by the Department through a motor vehicle record. The background story which led to the introduction of the DPPA is particularly imperative for the demonstration of the reactive nature of data protection in the United States. The main event leading up to the DPPA was the death of actress Rebecca Schaeffer in 1989.[346] An obsessed fan hired a private investigator to discover Schaeffer's private address. The investigator managed to obtain Schaeffer's address from the California Department of Motor Vehicles. The fan subsequently used the address to stalk and kill Schaeffer. Still, several years later, during a Senate Hearing on the Identity Theft Assumption and Deterrence Act in 1998, Special Agent Mari Riley described how the *Washington Post* issued a series of articles in March 1998 in which the Post elaborated on how various State and local government agencies released personal information to marketers, database managers, and other interested parties. The Post furthermore reported how numerous Department of Motor Vehicle Agencies provided personal information in the form of mailing lists. Interested parties paid a fee to request the DMV to conduct a customized search of driver's license and car registration records, which generally contain detailed personal data including unlisted addresses and medical conditions. One state agency earned approximately $12.9 million in revenue in exchange for motor vehicle agency generated mailing list information, according to the Post.[347]

For the private sector, the United States Congress introduced legislation in 1970 through the Fair Credit Reporting Act (FCRA), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies (see chapter 5). Other initiatives intended to protect personal information from individuals within the private sector include the Cable Communications Policy Act (CPPA) of 1984, which intends to protect the personal information of clients of cable service providers.[348] The CPPA requires cable service providers to inform their clients about the nature and the uses of the information collected about them. Disclosure of personal viewing habits of clients is prohibited through the CPPA, but disclosure about clients is permitted when such disclosure is "…necessary to render, or conduct a legitimate business activity related to, a cable service or other service provided by the cable operator to the subscriber."[349]

Four years later, the United States Congress passed the Video Privacy Protection Act (VPPA) of 1988. This initiative was a response to reporters who managed to obtain the videocassette rental data of Supreme Court Justice

---

[344] Pub. L. No. 104-191.
[345] 18 U.S.C. § 2721
[346] Electronic Privacy Information Center (EPIC). *The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record.* Available at: http://epic.org/privacy/drivers/ (last accessed July 12, 2010).
[347] Riley, M. (1998). Statement to the U.S. Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary. *The Identity Theft and Assumption Deterrence Act*, Hearing, May 20, 1998 (Serial 105 - 779): 11.
[348] Pub. L. No. 98-549, 98 Stat. 2794 (Jun. 19, 1984), *codified* at 45 U.S.C. 551
[349] *Ibid.*

Nominee Robert Bork.[350] The VPPA therefore prohibits the disclosure of titles of videocassettes which people have either bought or rented from videotape service providers. Whereas the content of the VPPA is largely irrelevant to the issue of financial identity theft, its background story is interesting to mention due to its expression of the 'reactive nature' of privacy policy in the United States.

For financial identity theft, the most relevant legal instruments with respect to data protection are the previously mentioned FCRA of 1970, the Fair and Accurate Credit Transactions Act (FACTA) of 2003 and the Gramm-Leach-Bliley Act (GLBA) of 1999. FACTA demands the truncation of credit card and debit card account numbers. FACTA specifically states how "...no person that accepts credit cards or debit cards for the transaction of business shall print more than the last 5 digits of the card number or the expiration date upon any receipt provided to the cardholder at the point of the sale or transaction."[351] This part of FACTA applies to merchants and is an important amendment in light of dumpster diving, a method used by perpetrators to obtain sensitive information to commit identity theft. The GLBA includes provisions established to protect the personal financial information of consumers maintained by financial institutions.[352]

Overall, the privacy framework established in the United States receives both support and criticism. Selected sources support the available framework present in the United States with regard to information privacy, or rather data protection. Jonathan M. Winer testified how "[u]nlike the EU's lax enforcement of its privacy directive, the U.S. systematically enforces its privacy laws. The U.S. also has a high level of self-regulation. U.S. regulators have issued detailed regulations governing privacy in the financial services sector, and they examined financial institutions for compliance with U.S. privacy laws."[353] Primarily based on a 2001 study conducted by Consumers International, Winer claims how "[o]ur system protects privacy in practice better than the EU system...We have a system in this country of regulation and enforcement that is very aggressive. You go over to the EU they have got soft guidelines, and they have got much less enforcement. They don't have regulations for the most part."[354]

Other arguments set forth by those in support of the privacy framework in the United States center around the importance of the market. Shaun A. Sparks claims how 'Internet consumers' in the United States receive similar protection to consumers in the European Union. Sparks furthermore states how the approach in the United States "...allows for the unfettered development of online business models..."[355] The importance of such development is used in support of self-regulation. Sparks writes how "[t]he argument for self-regulation is not an argument against all regulation; it is an argument that online businesses should have the freedom to expand the boundaries of a dynamic new medium without artificial limitations."[356] This argument in favor of self-regulation is familiar to the

---

[350] Solove (2004): 69.
[351] Pub.L. No. 108-159.
[352] Pub.L. No. 106-102, 113 Stat. 1338.
[353] Winer, J. M. (2001). Testimony to the U.S. House Subcommittee on Commerce, Trade and Consumer Protection of the Committee on Energy and Commerce. *The EU Data Protection Directive: Implications for the U.S. Privacy Debate*, Hearing, March 8, 2001 (Serial 107 – 19): 46-47.
[354] *Ibid*: 98.
[355] Sparks, S. A. (2000). The Direct Marketing Model and Virtual Identity: Why the United States Should Not Create Legislative Controls on the Use of Online Consumers Personal Data. *Dickinson Journal of International Law*, Vol. 18 (3): 544.
[356] *Ibid:* 550.

United States and returns in chapter 5 during the discussion of the introduction of Internet banking. Other important proponents of the available framework include Thomas M. Lenard and Paul H. Rubin.[357]

Other sources, on the other hand, criticize the information privacy framework in the United States. Fred H. Cate summarizes the framework in the United States as follows, "[t]he protection for information privacy in the United States is disjointed, inconsistent, and limited by conflicting interests. There is no explicit constitutional guarantee of a right to privacy in the United States."[358] Furthermore, he states that "[t]he U.S. privacy principles are silent on the enforcement of privacy rights against data collectors and processors, and the constitutional commitment to a government of limited powers, particularly when expression is involved, poses a substantial obstacle to the creation of a government privacy authority."[359] The European approach taken instead receives more favorable reviews when authors draw a comparison between both the United States and the European Union. Joel R. Reidenberg notes, "[w]hile there is a consensus among democratic states that information privacy is a critical element of civil society, the United States has, in recent years, left the protection of privacy to markets rather than law. In contrast, Europe treats privacy as a political imperative anchored in fundamental human rights. European democracies approach information privacy from the perspective of social protection."[360]

With regard to self-regulation, Jonathan P. Cody claims how such an approach received ample time to prove its effectiveness on the Internet. After three years, Cody claims, self-regulatory mechanisms have failed to catch on in the online environment. Unlike Sparks, Cody considers the approach in the United States to be void of the core principles expressed in the European Union.[361] Taken as a whole, Colin Bennett succinctly captures the failure of the information privacy framework in the United States when he writes, "[t]he approach to making privacy policy in the United States is reactive rather than anticipatory, incremental rather than comprehensive, and fragmented rather than coherent. There may be a lot of laws, but there is not much protection."[362] The reactive character of the approach with respect to privacy policy is certainly demonstrated through the introduction of the DPPA and the VPPA, and to some extent the manner through which the Privacy Act came about after Watergate and its political implications. The lack of a comprehensive approach to privacy policy appears to be the result of American fear for excessive government intervention in private activities and a dislike for broad industry regulations, according to Reidenberg.[363]

Another important criticism raised against the privacy framework in the United States is the Third Party Doctrine, which is an important limit of the

---

[357] Lenard, T. M. & P. H. Rubin (2009). *In Defense of Data: Information and the Costs of Privacy*. Technology Policy Institute Working Paper.
[358] Cate, F. H. (1997). *Privacy in the Information Age*. Washington, DC: Brookings Institution Press: 98.
[359] *Ibid.*
[360] Reidenberg, J. R. (2001). E-Commerce and Transatlantic Privacy. *Houston Law Review*, Vol. 38: 730 – 731.
[361] Cody, J. P. (1999). Protecting Privacy over the Internet: Has the Time Come to Abandon Self-Regulation? *Catholic University Law Review*, Vol. 48: 1183 – 1236.
[362] Bennett, C. J. (2001). 'Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?' in P. E. Agre & M. Rotenberg (eds.) *Technology and Privacy: The New Landscape*. Cambridge, MA: MIT Press: 113.
[363] Reidenberg, J. R. (1992). Privacy in the Information Economy: A Fortress or Frontier for Individual Rights? *Federal Communications Law Journal*, Vol. 44: 195 – 244.

Fourth Amendment right to unreasonable search and seizures. Once information is relinquished to a third party, such information no longer receives the protection of the Fourth Amendment rights. As a result, any information provided to third parties, whether banks or Internet Service Providers, is available to the government.

The Third Party Doctrine is a source of support and criticism. Solove provides an alternative proposal for the Third Party Doctrine which requires law enforcement to obtain probable cause in order to obtain access to information held by third parties.[364] Another alternative comes from Christopher Slobogin who argues in favor of a proportionality principle.[365] Slobogin criticizes the alternative introduced by Solove due to its 'overinclusive' nature, since Solove fails to distinguish between the types of information held by third parties and as such the proposal requires law enforcement to have probable cause for all information before they can gain access. The proportionality principle introduced and defended by Slobogin distinguishes between various categories of information. These include organizational vs. personal, private vs. public, and content vs. catalogic records.[366]

According to Stephen E. Henderson, the Third Party Doctrine is not the universal constitutional rule in the United States. Henderson notes how eleven States reject the Third Party Doctrine and provide some Fourth Amendment protections to information held by third parties.[367] Henderson provides a more nuanced approach to the Third Party Doctrine and identifies various factors which he considers relevant to the decision of whether law enforcement ought to have access to the information. The first factor is the purpose of disclosure. Henderson writes how if the disclosure is necessary for societal participation, then such disclosure weighs in favor of restricted access to the information by law enforcement officials.[368] The second and third factors focus on the personal nature and the amount of the information respectively.

Whereas Solove, Slobogin, and Henderson all aim to develop an alternative to the practice of the Third Party Doctrine in contemporary society, Orin S. Kerr defends the Third Party Doctrine. Generally, Kerr states how those whom have attacked the Third Party Doctrine have failed to observe its benefits. And these critics have also in turn overestimated the weaknesses of the Doctrine. More specifically, Kerr writes how "[t]he third-party doctrine serves two important roles: blocking substitution effects that upset the technological neutrality of Fourth Amendment law and furthering clarity of Fourth Amendment rules."[369]

The criticism against the sectoral approach used in the United States does not automatically lead to support for a comprehensive federal omnibus privacy law, such as the European Union maintains. Paul M. Schwartz describes the possible negative effect of the introduction of a federal omnibus information privacy law in the United States. Throughout the years, individual States "...have been especially

---

[364] Solove (2004).
[365] Slobogin, C. (2005). Transaction Surveillance by the Government. *Mississippi Law Journal*, Vol. 75: 139 – 192.
[366] *Ibid.*
[367] Henderson, S. E. (2006). Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search. *Catholic University Law Review*, Vol. 55: 373.
[368] Henderson, S. E. (2007). Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too. *Pepperdine Law Review*, Vol. 34 (4): 989.
[369] Kerr, O. S. (2009). The Case for the Third-Party Doctrine. *Michigan Law Review*, Vol. 107: 561 – 602.

important laboratories for innovations in information privacy law."[370] As laboratories States have played a pivotal role in the evolution of information privacy law, particularly due to the ability of the various States to identify a need for legislation early on. Furthermore, States have demonstrated innovative approaches to challenges posed by societal changes, according to Schwartz, and through the varying nature of approaches States have also allowed for simultaneous experimentation which leads to a more insightful look on the most promising types of information privacy law. The emphasis of the argument set forth by Schwartz is on the relation between the Federal nature of the United States and its implications for legislation. A Federal omnibus privacy law may negatively impact the benefits of individual state action due to the issue of preemption. The innovative character of individual state action often increases the level and quality of consumer protection. Preemption then trumps the state's ability to offer heightened consumer protection and to experiment with more innovative approaches than available at the Federal level.

Another concern expressed by Schwartz is the potential that the Federal government is unlikely to revisit the statute to amend certain aspects. This could pose a problem because of the continuously evolving landscape of information privacy. Especially as societal developments introduce new risks and challenges for consumers.

Patricia L. Bellia partially criticizes the argument set forth by Schwartz. In her contribution to the debate, she writes "[s]trong preemption is unproblematic if the resulting regulation strikes the right privacy balance; the real concern is that federal law will be broadly preemptive and will under regulate."[371] While Bellia shares this apprehension, she claims it is not a concern of federalism or comprehensive federal legislation. "I am not confident that we can credit state experimentation with privacy successes or that we can blame federalization for its failures."[372]

3.3.2 The Netherlands

On the other side of the ocean, the privacy and data protection debate began during the sixties. The initial debate mainly took place outside of the public eye. A television show about the Second World War accompanied by various publications describing the role of the near perfect record-keeping activities used to isolate and subsequently eradicate the Jewish population slowly began to illustrate potential problems.[373] The government nevertheless maintained a positive outlook on the possibility of automated record-keeping and yearned for the most efficient usage of such tools. To accomplish its mission, the Minister of the Interior initiated a research committee to investigate the redesign and automation of public record keeping. In particular, the government expressed interest in the possibility and desirability of the usage of other methods and tools to conduct record-keeping.[374] The government also desired to discover, through the Committee, how to most efficiently guide the communication of information

---

[370] Schwartz, P. (2009). Privacy and Preemption. *Yale Law Journal*, Vol. 118: 916.
[371] Bellia, P. L. (2009). Federalization in Information Privacy Law. *Yale Law Journal*, Vol. 118: 900.
[372] *Ibid.*
[373] Overkleeft-Verburg, G. (1995). *De wet persoonsregistraties: norm, toepassing en evaluatie*. Zwolle: Tjeenk Willink.
[374] Commissie Simons (1968). *Rapport inzake automatisering verstrekking van inlichtingen uit de bevolkingsregisters*. 's-Gravenhage: Staatsuitgeverij.

between the information provider and the agencies receiving the information. Several years after its installation, in 1968, the Committee Simons published its report and provided several recommendations.

In its report, the Committee claims how it would be a testament to bad policy if the government were to fail to fully profit from the benefits offered through modern electronic machines for administrative purposes.[375] Furthermore, the Committee emphasizes the increased benefit of massive information collection and storage, and uses this idea as a lead into its recommendation for the establishment of a central database.[376] Such centralized data collection, storage and processing requires a tool to facilitate its usage and efficiency. The Committee therefore introduces an administrative number which assists the codification of the information maintained by the central database. This was to also facilitate the information exchange between the information providers and the recipients. And makes information easier to store and find. The usability of the number is most extensive when all government agencies along with a selected group of private sector organizations are allowed to use the number.

Throughout the discussions of its recommendations, the Committee continuously emphasizes the efficiency and convenience benefits attached to the introduction of a central database and an accompanying administration number for citizens. The security aspect is mentioned more as an afterthought than as an essential element of the system. The Committee identifies the sensitive nature of the information maintained in the database and claims the government maintains the responsibility to ensure the safety of the information and to prevent access to third parties.

After the publication of its findings and recommendations, the government called upon another committee to follow up on the research conducted by the Committee Simons. The follow up was to investigate the desirability of the introduction and broad implementation of a general administrative number.[377] The Committee Westerhout expressed its support for the introduction and subsequent implementation of a general administrative number for all citizens in the Netherlands.

Parallel to these committee developments began the preparations for the census of 1971. The preparation of the 1971 Dutch census, which occurred during the summer of 1970, became the instigator for the subsequent public outrage. Through reports from a more critical media, the public became interested and a sense of unrest commenced. As a result, the period leading up to the 1971 census became one of awareness raising, both among the public as well as the media.[378] The census discussion placed the topic of privacy firmly on the map. According to Frank Kuitenbrouwer, "[o]ur country lost its innocence on Sunday 28 February 1971 when precisely at midnight the official start sign of the fourteenth general population census (since 1829) rang."[379] The census inspired an enormous number of action groups who engaged in protests. Kuitenbrouwer notes how it is not as surprising as it may initially appear that the statistical research caused such public

---

[375] *Ibid:* 16.
[376] *Ibid.*
[377] Commissie Westerhout (1970). *Rapport inzake registratie van persoonsgegevens*. 's-Gravenhage: Staatsuitgeverij.
[378] Sentrop, J. W. (1985). *Privacy-bescherming in Nederland*. Deventer: Van Loghum Slaterus.
[379] Kuitenbrouwer, F. (1991). *Het recht om met rust gelaten te worden*. Amsterdam: Balans: 65. Translation van der Meulen.

outrage and unrest. Statistical research can lead to statements about certain groups of people which means individuals within those groups can experience the consequences of such conclusions. While the individual may enter anonymously, the results become personal.[380]

Due to the protests which incorporated doom scenarios as portrayed in George Orwell's *1984* along with Kafka's *The Trial*, emotions or rather emotion-filled speech dominated the debate.[381] Public officials welcomed this 'emotional character' because they claimed how rational reasoning was absent from the discussion since emotions played such a vital role. Furthermore, the examples used during the discussions of the contested developments and their associated dangers mainly came from the United States. The government front subsequently managed to easily dismiss these examples as 'horror stories from the United States.'[382] In addition, the debate surrounding the incorporation and subsequent usage of personal identification numbers often included references to the personal identification card used during the Second World War. Public officials perceived and labeled this reference yet again as emotional.

Still, the interest of the public created sufficient political pressure and momentum to force the political arena to investigate the potential for dangers associated with the automation of personal record-keeping. On 16 March, 1972, the Minister of Justice introduced the State Committee Koopmans. During the induction of the Committee, the Minister of Justice described how only recently the potential for invasions of privacy through the use of the computer came to light. In particular, the ability to combine various sources of personal information along with the opportunity to access such personal information from a distance are risks which remained unknown until the early seventies, according to the Minister.[383] The potential dangers formed the primary reason for the establishment of the Committee and its assignment to conduct background research. The Minister furthermore notes how the potential dangers associated with accumulating, storing and processing personal information should be analyzed both with regard to the public as well as the private sector. The mere possession, according to the Minister, of information about others can provide individuals or agencies with the power to significantly influence the lives of others. The government gave the Committee Koopmans considerable freedom to elaborate upon the assignment as the Committee saw fit for the occasion. Despite the freedom, the government emphasized the need to examine the dangers associated with automated registration systems. In its final report, the Committee acknowledges the desirability for additional legislation with regard to the protection of personal information in automated systems.[384]

Parallel to the discussion on proposing legislation to develop a data protection framework, the government introduced an amendment to the Dutch Constitution on February 17, 1988 which officially recognized the right to privacy.[385] This

---

[380] *Ibid.*

[381] Sentrop (1984): 42.

[382] *Ibid*: 42 – 43.

[383] Commissie Koopmans (1976). *Eindrapport van de Staatscommissie Bescherming Persoonlijke Levenssfeer in verband met Persoonsregistraties*. 's-Gravenhage: Staatsuitgeverij.

[384] *Ibid.*

[385] Article 10 of the Dutch Constitution states (translation van der Meulen):
1. Everyone has the right to respect of his personal privacy.
2. The law sets rules to protect the personal privacy in connection to the registration and provision of personal information.

amendment came years after the peak of the political debate on privacy. This peak occurred during the mid-seventies when the Prime Minister described the right to privacy as an essential condition for a humanitarian existence and as a fundamental principle of the rule of law.[386] This description of privacy therefore required its incorporation into the constitution in an effort to demonstrate its fundamental importance to the State and its citizens.

After years of political discussion and research, the government introduced the *Wet persoonsregistraties (WPR)* or the Dutch Data Protection Act, which came into effect on July 1, 1989. This extended time frame between the publication of the conclusions of the Committee Koopmans and the actual introduction of legislation with respect to data protection is partly the result of alternative methods of data protection implementation. The Netherlands used most of the seventies and the eighties to experiment with self-regulation and sectoral legislation. The Bureau for Credit Registration and the direct marketing sector developed codes of conduct in 1965 and 1975 respectively in the absence of government regulation for data collection and processing. In addition, banks, insurance corporations, and publishers also maintained codes of conducts to guide their data protection efforts. Peter Blok describes how these two decades can be observed as an experiment of American implementation mechanisms in a Dutch context.[387] The existence of sectoral laws, before the introduction of the WPR, demonstrates how the Netherlands did have a range of applicable laws which regulated a number of important data registration systems.[388]

Despite the experimentation, the actual development of an overarching data protection act occurred slower than anticipated. This delay occurred despite the proclamation of the Minister of Justice about how the design of a data protection act received the highest priority within the Department.[389] As Blok notes, the legislative process clearly did not demonstrate the same pace as the technological developments. Pressure from outside sources, such as developments within the Council of Europe, increased the necessity for the introduction of a data protection act. The initial design of the data protection act proved remarkably similar to the recommendations made by the Committee Koopmans, which led to an increased level of irritation about the delay of the design.[390] The initial design of the data protection act did not distinguish between the public and the private sector and primarily focused on automated personal data registration. Various sources voiced their criticism about the bill.[391]

The second attempt introduced by the Minister of Justice on July 25, 1985 provided a radically different bill. Despite the differences, the bill maintained the original ideas of the Committee Koopmans. The bill maintained the character of an omnibus law and introduced a central supervisory organ. The revised bill did distinguish between the public and the private sector. The bill still proved applicable to both sectors, but obligated the public sector to implement a

---

3. The law sets rules with respect to claims made by people to investigate the personal information registered about them and the usage of such information, as well as improvement of the relevant information.

386 Blok, P. (2002). *Het recht op privacy; Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*. Den Haag: Boom Juridische Uitgevers.

387 *Ibid:* 139.

388 *Ibid.*

389 *Ibid:* 143.

390 *Ibid.*

391 *Ibid:* 144.

framework of self-regulation whereas the bill merely encouraged the private sector to implement self-regulatory mechanisms.

Party as a result of developments at the European level, the WPR became the object of extensive evaluation. The Ministry of Justice initiated two evaluations. The first focused on the effectiveness of the law and paid particular attention to the incorporated system of self-regulation within the Act.[392] The second evaluation shed a different light on the WPR through its social scientific analysis of the law.[393] Both research evaluations published particularly negative conclusions about the effectiveness of the WPR.

The legal evaluation concluded how there is a lack of compliance with the administrative mandates anchored in the law. Especially the mandate to notify the central supervisory organ of data registration activities is approached and observed as "a one-time obligation of a purely administrative manner."[394] Many ignore the mandate and fail to notify the Registration Chamber altogether. The initial period of implementation demonstrates a quantitative peak of notifications. According to Overkleeft-Verburg, "[t]he curve of notification shows that observance of the obligation of notification was concentrated in the first phase of the implementation of the WPR, the period from January 1st 1990 to July 1st 1991."[395] Soon thereafter, notifications from the private sector quickly dropped, whereas for the public sector the decline proved more subtle and gradual.

Besides the quantitative neglect, the quality of the notifications also failed to meet the standards as identified by the WPR. Overkleeft-Verburg calls the overall results with respect to notification and self-regulation disappointing. "It is ignored by many, or only taken as a token of obligation. Even an active enforcement policy by the Registration Chamber cannot be expected to change this radically."[396]

The social scientific evaluation captured the essence of the WPR when the authors write, "[a] law for outsiders and a law for insiders: this is how the DPA can be characterised. During its five-year existence, this act has generally eluded the attention of those it was intended for: the data subjects. Outsiders are those who in every day terms have to work with a rules system that is complicated, difficult to access and substantially only usable in a limited way. Therefore, it remains an act for outsiders."[397] The main aim, according to the authors, especially in light of societal developments, ought to be to make the 'outsider' an 'insider' with respect to the protection of personal data and the protection of autonomy and identity.

The sequel to the WPR, *Wet bescherming persoonsgegevens* (Wbp), came about in part as a result of the negative evaluations. The government acknowledged the inadequacies of the WPR and also realized the need for change. The other main development which compelled the government to initiate new legislation was the introduction of the Directive 95/46/EC of the European Union. Just as developments with respect to data protection, or information privacy, occurred in

---

[392] Overkleeft-Verburg (1995).
[393] Prins, J. E. J., van de Donk, W. B. H. J., van Duiveboden, H. P. M., ten Have, K., Nouwt, J., Vorselaars, H. A. C. M. & S. Zouridis (1995). *In het licht van de Wet Persoonsregistraties: zon, maan of ster?* Samson Bedrijfsinformatie bv: Alphen aan de Rijn.
[394] Overkleeft-Verburg (1995): 575.
[395] *Ibid.*
[396] *Ibid*: 704.
[397] Prins *et al.* (1995): 418.

the Netherlands and the United States, other governmental organs also observed changes in society and responded accordingly. The Directive 95/46/EC is a product of these observations and concerns. David Smith states how "[t]he EU Data Protection Directive is designed to harmonize European laws and to remove barriers to the flow of information within Europe. It essentially takes the Council of Europe Convention further, makes it a mandatory requirement, and modifies it in relation to EU member states."[398] Smith refers to the Council of Europe Convention which finds its roots in the early 1970s as the Council of Europe recognized the need to "establish a framework of specific principles and norms to prevent unfair collection and processing of personal data."[399] This conclusion came as a result of the rapid changes with regard to electronic data processing and the introduction of extensive data banks during the 1960s. During the early 1970s, the Council adopted Resolutions (73) 22 and 74 (29), which are viewed as the first building blocks of the current supranational data protection regime. These resolutions introduced principles for the protection of personal data in automated data banks both in the private and the public sector.[400]

The Council's main aim for the resolutions was to inspire national legislation of a similar fashion. Through the development process of the resolutions, however, the Council came to realize how thorough data protection could only be effective through the inclusion of both national and international legislation and enforcement. In 1972, the Conference of European Ministers of Justice concurred with the Council's conclusion. After several years of negotiation, the Council presented the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981. Several years later, in 1990, the European Commission wrote "[t]he increasingly frequent recourse to the processing of personal data in every sphere of economic and social activity and the new data-exchange requirements linked to the strengthening of European integration necessitate the introduction in the Community of measures to ensure the protection of individuals in relation to the processing of personal data and to enhance the security of information processing in the context, notably, of the development of open telecommunications networks."[401] The need for a separate Directive within the European Union therefore became apparent. Especially since the Commission also received calls from the European Parliament to take action through a proposal for a directive to harmonize laws across the Member States since 1976.[402] Some years after 1976, the Commission recognized the need for data protection across all Member States in the European Union. As such the Commission encouraged all Member States to ratify the Council of Europe Convention, for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, before the end of 1982.[403]

---

[398] Smith, D. (2001). Statement to the U.S. House Subcommittee on Commerce, Trade and Consumer Protection of the Committee on Energy and Commerce. *The EU Data Protection Directive: Implications for the U.S. Privacy Debate*, Hearing, March 8, 2001 (Serial 107 – 19): 14-15.

[399] Council of Europe (n.d.). Background. Available at http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/background/11Background.asp (last accessed July 12, 2010).

[400] *Ibid.*

[401] Commission of the European Communities (1990). Commission communication on the protection of individuals in relation to the processing of personal data in the community and information security. Brussels September 13, 1990.

[402] *Ibid.*

[403] *Ibid.*

The Commission, however, also acknowledged the need to go one step beyond recommending Member States to ratify the Council's Convention. As the Commission stated in 1990, "[t]he diversity of national approaches and the lack of a system of protection at the Community level are and obstacle to completion of the internal market."[404] Especially during a time when the cross-border flow of data became more important for businesses, research bodies and the cooperation of various authorities in the Member States it was essential to ensure the protection of the fundamental right of all EU citizens to privacy. The Strasbourg Council of 8 and 9 December 1989 also emphasized the primary need to ensure the protection of individuals in personalized data banks as part of the promotion of the movement of people and products. The growing pressure assisted in the introduction of the ultimate product which came about in 1995 through the Directive 95/46/EC. The Member States received the mandate to implement the Directive at the national level within three years after its introduction.

The Dutch government failed to meet its deadline in October 1998. Instead, the government only presented the first draft of the bill in February 1998.[405] The bill received fierce criticism from various stakeholders, especially since they all held different, and at times, conflicting interests.[406] Due to the complications associated with the criticism, the Minister decided in November 1998 to introduce substantial changes to the bill. These changes once again led to criticism from unhappy stakeholders which forced the government to spend the following year in search of a compromise.[407] Certain changes needed to be reversed as a result of objections posed by the Lower House. Perhaps in an effort to meet the needs of many stakeholders, the government developed a complicated piece of legislation, which made its unpopularity soar.[408]

The Wbp came into force on September 1, 2001. The Wbp differs from its predecessor in a number of respects. The most prominent difference appears to be that the legislative focus extends beyond the mere registration of personal data to include any and all ways of dealing with personal data such as collecting, organizing, adjusting, changing, spreading, processing, and destroying personal information.[409] This expansion is a direct response to societal developments and demands with regard to the handling of personal information. Especially since the mere registration of such information was no longer the central aspect of personal information and its protection.[410] Other differences include the elimination of the distinction of personal data protection in the public and the private sector.

The main elements, on the other hand, of the Wbp coincide with its predecessor and the ideas discussed by the Committee Koopmans. The Wbp introduces several open standards with regard to data protection which require individual organizations to introduce specific self-regulation. Due to the elimination of the distinction between the sectors, the standards became even broader than in the WPR. The law guarantees the right to all data subjects to view

---

[404] *Ibid:* 4.
[405] *Kamerstukken II* 1997 – 1998, 25 892, nr. 1-2.
[406] See Prins, J. E. J. & J. M. A. Berkvens (2007). 'De Wet Bescherming Persoonsgegevens,' in J. E. J. Prins & J. M. A. Berkvens (eds.) *Privacyregulering in theorie en praktijk*. Deventer: Kluwer: 25 – 46.
[407] *Ibid.*
[408] *Ibid.*
[409] Blok (2002): 150.
[410] *Ibid.*

and correct their personal information. And data subjects can also resist the processing of personal data in the realm of direct marketing.

Since Article 80 of the Wbp calls for an evaluation, the Minister of Justice commissioned a dual evaluation in 2007.[411] The first evaluation was to discover the 'bottlenecks' of the Wbp based on a literature study. The second evaluation, on the other hand, was to focus on a more empirical analysis of the law based on field research. The literature study which focused on the bottlenecks provided the following conclusions.[412] The first bottleneck is the lack of clarity provided by the law itself. This is because such unclarity complicates compliance and might obstruct technological developments. This conclusion is not shared by all authors of the evaluation since others support the 'broad' character of the law and as such view the preservation of such broadness as imperative. The omnibus nature of the law, according to the authors, leads to challenges related to the complexity of interpretation and a lack of flexibility. Despite these challenges, the omnibus nature of the law is still preferred over a sectoral approach.[413]

The second evaluation, which maintained a more empirical character, came about in September 2008.[414] The results indicated how the implementation of the legislation was yet to be fully realized. The image developed as a result of the research conducted demonstrated how the law was not really alive in legal practice.[415] The open standards required time to be more specifically defined. Furthermore, because of the different challenges encountered in various sectors, specification of standards required jurisprudence and context specific knowledge. The evaluation states how the Wbp is a young piece of legislation. Yet, the team also recognizes the existence of its predecessor, which means its youth is hardly an argument in support of its disappointing implementation. The mere existence of open standards as a core element of the WBP is in itself not a problem or a stumbling block. Such an existence becomes problematic when the development of specific norms and codes of conduct fails to occur in the various relevant branches.[416] At the time of the evaluation, approximately half of the relevant organizations had established a privacy code; as such, the other half had not.

The role of the Data Protection Authority (DPA) received mixed reviews.[417] Whereas some expressed their contentment with regard to the work of the DPA, in particular the publications, others desired more from the agency. Those who wanted more action from the DPA specifically wanted the agency to play a larger role in compliance assistance, information delivery, and advice. There appears to be a significant demand for assistance with regard to the interpretation and explanation of the law.

In January 2008, the deputy Minister of Justice along with the Minister of the Interior installed the Committee Brouwer-Korf in order to assess the possibilities

---

411 *Kamerstukken II* 2006 – 2007, 31 501, nr. 1.

412 Zwenne, G. J., Duthler, A-W., Groothuis, M., Kielman, H., Koelewijn, W. & L. Mommers (2007). *Eerste fase evaluatie Wet bescherming persoonsgegevens Literatuuronderzoek en knelpuntenanalyse*. Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC).

413 *Ibid.*

414 Winter, H. B., de Jong, P. O., Sibma, A., Visser, F. W., Herweijer, M., Klingenberg, A. M., & H. Prakken (2008). *Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk*. Den Haag: Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC).

415 *Ibid.*

416 *Ibid.*

417 *Ibid.*

for a faster and more responsible method of data exchange among various parties including aid workers, crime fighters and prevention workers.[418] The Committee Brouwer-Korf speaks of an intensification of the government's battle with respect to small and large forms of criminality. The worldwide fight against terrorism functions as a driver for legislation where the collective security forms the primary objective. Others, including citizens and the private sector, also appear to demonstrate a growing demand for a more active state to establish a secure society and to eradicate unsafe situations. Privacy and security have become opposite concepts during the intensification of the government's role as protector in its fight against all forms of criminality. The Committee describes a situation throughout which privacy and security are used as catch-all phrases without the necessary specification of what either concept implies throughout the debate. The concept of security appears to be claimed by those who wish to protect society from all potential risks, including terrorism, crime, and abuse of personal data.[419] Privacy, on the other hand, appears to be defended by those who aim to secure the democratic values required for a society to thrive.[420]

The most accurate reflection of the debate set forth by the Committee is their description of the one sided usage of both concepts. Such a one sided depiction of privacy and security leads to a situation where the concepts become enemies rather than cooperative partners in a complex society.[421] Discussions speak either of security or privacy rather than presenting a more overarching approach which encompasses both aspects. This is problematic in light of the position of collective security as a top priority for public policy.[422] The Committee eloquently describes how "[t]he depiction of security therefore occurs in absolute terms whereas privacy remains relative and therefore adjustable to the other interests at stake in society. Law enforcement along with various politicians focus on the less positive aspect of privacy which generally hinders certain actions they wish to take. Such less positive aspects are, however, the cost of liberty. To treat privacy or data protection as a conditional right opens the door to abuse."[423]

The Committee acknowledges the lack of attention granted to the need to strike a meaningful balance between privacy and security. More recently, the idea of striking a balance has demanded more attention from the political arena through the publication of academic research.[424] The segregated debate about privacy and security fails to stimulate an understanding or realization about how the right to privacy in itself is a form of security, albeit individual security.

All of the various developments through the past decades have increased the tension between privacy and security. The Committee sets forth six general criteria which ought to be applied to situations where a balance must be found between security and privacy. These six criteria include:

1 Transparancy, unless…

---

[418] Commissie Brouwer-Korf (2009). *Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer.*
[419] *Ibid:* 15.
[420] *Ibid:* 16.
[421] *Ibid.*
[422] *Ibid:* 16.
[423] *Ibid.*
[424] See for example Muller, E. R., Kummeling, H. R. B. M. & R. P. Bron (2007). *Veiligheid en privacy: Een zoektocht naar een nieuwe balans,* Den Haag; Vedder, A., Van der Wees, L., Koops, E. J. & P. De Hert (2007). *Van privacyparadijs tot controlestaat*, Rathenau Instituut.

2 Select before you collect – the main aim of this condition introduced by the Committee is to minimize data collection down to the bare necessity. The Committee also pleads for a risk assessment before data is collected and stored by officials.
3 In case necessary for security purposes, you must share – If it is clear individuals are in danger or at risk of being endangered, and the sharing of personal information can reduce the danger or its accompanying risk, then relevant officials must share personal information.
4 Ensure integrity of data, systems, and the handling of users – During the development of systems, privacy-related risks must be taken into consideration during the early stages.
5 Provide education and facilitation – Best and good practices must be available for those out in the field.
6 Ensure compliance and internal supervision.

In its reaction to the report presented by the Committee Brouwer-Korf, the government recognizes the limited effectiveness of the current legal framework available. The government therefore presents several proposals to approach the 'causes' of the problem.[425] These proposals are diverse and include both legal and incentive related policy. This is, according to the government, a first step toward a new approach in its effort to protect the privacy of the citizens of the Netherlands. To carry out these proposals, the government plans to install a 'program organization' which shall include representatives of all relevant parties. Furthermore, the government intends to introduce amendments to the current data protection law, which shall include the recommendations set forth by the Committee Brouwer-Korf, the evaluation report of the data protection law, and input received by other parties such as the DPA.

During the parliamentary debate in response to the reaction offered by the government, certain members of the Lower House referred to critical aspects of the reaction. Alexander Pechtold reflected on the select before you collect recommendation set forth by the Committee. He describes how various intelligence agencies are nearly drowning in the information they collect and there is a low 'gold to garbage ratio' as the Americans say.[426] Pechtold states how in response to the recommendation the government claims it only collects information which is absolutely necessary to accomplish an objective. This reaction, according to Pechtold, lacks self-criticism especially in light of the collection of SWIFT and PNR data.

This remark is of vital importance for the overall approach to and treatment of data protection, including data collection, processing, and storage by government agencies. As the above demonstrates, the primary focus, when the computer came into the picture, was on the capabilities of automated systems to improve record keeping activities. The potential vulnerabilities only received attention as a result of public pressure. Moreover, the tension between collective and individual security, or privacy, is evident, especially in light of the continuous pressure put on data protection requirements and the near obsession expressed by government agencies to collect and store personal information.

---

[425] *Kamerstukken II* 2009 – 2010, 31 051, nr. 5.
[426] *Kamerstukken II* 2009 – 2010, 31 051, nr. 7.

3.4 Data Security Breach Legislation

3.4.1 United States

Changes in the privacy and data protection landscape inevitably led to a search for additional means of protection. The general story traces the historical background of data security breach notification initiatives in the United States back to 2002, when hackers gained access to the State of California's government payroll database, which contained sensitive personal information of over 250,000 state employees.[427] The members of the California legislature were among the employees whose personal information was exposed through the data security breach. According to Benjamin Wright the onset for the notification requirement occurred because "[m]any employees, including the legislators, felt the California government was too slow to notify them about the burglary."[428] As a result, the State of California passed two separate initiatives in 2002. First, the California Security Breach Information Act[429] which requires any company which stores customer data electronically to notify its California customers of a security breach to the company's computer system when the company knows or has reason to believe that unencrypted information about customers has been disclosed. The second law, commonly known as the California Financial Information Privacy Act,[430] establishes new limits on the ability of financial institutions to share nonpublic personal information about their customers with affiliates and third parties.

The actual story, as told by California State Senator Joseph Simitian, demonstrates the strange confluence between politics and news media. In his own words, Simitian writes how "Assembly Bill 700, the security breach notification legislation…is the law today only because of a spelling error, an afterthought, an unrelated concern with digital signatures, a page three news story, the rule of germaneness, the intellectual quirks of a lame-duck Senator, the personal experiences of 120 State legislators, and another bill altogether, Assembly Bill 2297."[431] The California Security Breach Information Act became the first of its kind and paved the way for many successors. These successors began after the media extensively reported on a data security breach at ChoicePoint in 2005 (see chapter 7). Consumers in California received notifications of the incident because of the statutory obligation imposed as a result of the California Security Breach Information Act, however the company refused to notify residents of other States which created the controvery that led to the spread of breach notification obligations.

Throughout the years, the number of States introducing data security breach notification requirements continued to grow. As of December 9, 2009, 45 States, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. Proposals for legislation at the Federal level of government are

---

[427] Wright, B. (2004). Internet Break-ins: New Legal Liability. *Computer Law & Security Report*, Vol. 20 (3): 171-174.
[428] *Ibid:* 171.
[429] California Civil Code § 1798.82.
[430] California Civil Code § 1798.29.
[431] Simitian, J. (2009). How a Bill Becomes a Law, Really. UCB Security Breach Notification Symposium, March 6, 2009. Speech available at: http://www.btlj.org/data/articles/24_3/24_3_1.pdf.

presently under consideration. On December 8, 2009 H.R. 2221 the Data Accountability and Trust Act passed in the House of Representatives. The Act requires the Federal Trade Commission to promulgate regulations which require each person engaged in interstate commerce that owns or possesses electronic data containing personal information to establish security policies and procedures.[432] Furthermore, the Act also authorizes the FTC to require a standard method or methods for destroying obsolete non-electronic data, and to require information brokers to submit their security policies to the FTC in conjunction with a security breach notification or after a request issued by the FTC. Moreover, the Act requires the FTC to conduct or require an audit of security practices of information brokers when a breach occurs which the broker must issue a notification of. The Act also authorizes additional audits after a breach. With respect to information brokers, the Act requires them to "…(1) establish procedures to verify the accuracy of information that identifies individuals; (2) provide to individuals whose personal information it maintains a means to review it; (3) place notice on the Internet instructing individuals how to request access to such information; and (4) correct inaccurate information."[433] Other aspects of the Act prescribe procedures for notification to the FTC and affected individuals of information security breaches, and set forth special notification requirements for breaches.[434] If the Data Accountability and Trust Act also manages to successfully pass in the United States Senate, then its provisions shall preempt all State legislation with regard to data security breach notification.

Other Federal attempts with regard to data security breach notification occurred several years ago in 2005 when the FFIEC agencies issued their Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice. Satish M. Kini and James T. Shreve describe how, "[i]n brief, the Security Guidelines required banks to adopt comprehensive, risk-based information security programs designed to ensure the confidentiality of customer information, to protect against anticipated threats to such information, and to protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to customers."[435] This approach differs from the Californian approach, according to Schwartz and Edward J. Janger, since the guidelines set forth an idea where the breach letter ought to be send out to the applicable public when the likelihood of harm is significant.[436] This demonstrates the diversity in approaches with regard to data security breach notification.

Schwartz and Janger identify three different models. These include the model one which refers to statutes such as the Californian Security Breach Information Act. In model one, the threshold for notification is low. And the notification letter send to the victim must indicate the source of the breach. Schwartz and Janger describe model one as a pure notification model since a coordination structure which oversees the notifications is absent. The second model identified by

---

[432] See http://www.govtrack.us/congress/bill.xpd?bill=h111-2221 (last accessed July 12, 2010).

[433] *Ibid.*

[434] See http://www.govtrack.us/congress/bill.xpd?bill=h111-2221&tab=summary (last accessed July 12, 2010).

[435] Kini, S. M. & J. T. Shreve (2006). Notice Requirements: Common Themes and Differences in the Regulatory and Legislative Responses to Data Security Breaches. *North Carolina Banking Institute*, Vol. 10: 89.

[436] Schwartz, P. & E. J. Janger (2007). Notification of Data Security Breaches. *Michigan Law Review*, Vol. 105: 913 – 984.

Schwartz and Janger is the paradigm followed by the Interagency Guidelines. This model provides for greater flexibility for organizations through a two-tier approach. The first tier concerns notification to the oversight agency of the financial institution. Such notification maintains the same low threshold as model one. The difference between both models rests with the threshold introduced for consumer notification. This threshold is higher for the interagency guidelines, as noted above. The third model is a response to and as such an alternative for the approach introduced through the interagency guidelines. The Chicago Federal Reserve Board (FRB) suggested the idea of an intermediary third party in response to the issued guidelines. Such a trusted third party is to coordinate the response after a security breach and also alleviate the disincentive of disclosure. Schwartz and Janger note how "[t]his third model highlights the fact that breach notification serves both an ex ante and an ex post function."[437]

The spread of data security breach notification initiatives across the United States demonstrates their popularity as a means to provide for additional protection of consumers. This popularity stems from a selection of arguments set forth by proponents about the benefits and the necessity of such notification. These arguments in favor of notification focus on both consumers and the organizations which maintain their personal information. With respect to consumers, proponents reason how notification provides them with the necessary knowledge to take action in an effort to reduce the risk of identity theft.[438]

With respect to the organizations, the requirement to notify provides them with an incentive to prevent the occurrence of data security breaches through increased information security. This is because theoretically organizations want to prevent the potential reputation damage which might come about after sending the required notification. Such anticipated improved information security subsequently leads to a reduced opportunity for perpetrators of financial identity theft to access personal information. As Lilia Rode states, "[t]he duty to notify consumers about security breach inflicts tremendous costs on businesses. These costs inevitably induce behavioral changes that result in more sound privacy policies and improved data-security safeguards—thereby reducing identity theft."[439] The Government Accountability Office (GAO) also notes in a more hesitant manner how "[r]equiring consumer notification of data breaches may encourage better data security practices and help deter or mitigate harm from identity theft."[440]

Another argument made in favor of a statutory obligation to provide notification of a data security breach is the ability to collect data on security breaches in an effort to develop a more coherent picture about the events themselves.[441] This includes both quantitative information, such as data on the prevalence of security breaches, but also qualitative data about the background of the breach and the vulnerabilities which led to its occurrence. This argument is less prevalent in the literature, but deserves attention especially since such

---

[437] *Ibid:* 934.

[438] See for example Turner, M. (2006). Towards a Rational Personal Data Breach Notification Regime. *Information Policy Institute.*

[439] Rode, L. (2007). Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security. *Houston Law Review*, Vol. 43 (5): 1634.

[440] Government Accountability Office (GAO) (2007b). *Personal Information: Data Breaches are Frequent but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*: 6.

[441] Anderson, R., Böhme, R., Clayton, R. & T. Moore (2008). *Security, Economics, and the Internal Market*. Report commissioned by the European Network and Information Security Agency (ENISA).

information about breaches can provide assistance in the examination of areas of improvement with respect to information security.

Just as data security breach notification initiatives receive support, such initiatives also become the source of ample opposition. This opposition is posed both against the general idea of notification but also against the particulars of certain approaches, such as the threshold of notification maintained by the legal framework. The effectiveness of notification in light of consumer protection and empowerment is called into question. Thomas M. Lenard and Paul H. Rubin write "…in the best of circumstances, notification means that consumers might be able to respond more quickly to identity theft, not to avoid it altogether."[442] This conclusion is based on the inability of consumers to prevent or otherwise reduce the occurrence of financial identity theft once perpetrators manage to access the necessary personal information. As a result, the best case scenario is earlier detection in an effort to reduce the consequences of identity theft. This is nevertheless recognized by other sources and used to support notification rather than oppose its existence. Lenard and Rubin's opposition is still relevant due to the statements made by others.[443]

Elizabeth L. Garner expresses other concerns about the effective nature of notification for consumers. Garner states how "[b]reach notifications have the potential to be the next credit card junk mail—the piece of mail received two to three times a week, which is ripped up immediately upon receipt with no attention paid to its contents."[444] Michael G. Oxley expresses similar worries when he states, "[o]ne of my concerns in this regard is that given the dramatic rise in recent reports on data breaches, there will be a headlong rush toward notification in every instance. When no evidence surfaces to indicate that their information has been misused, consumers may begin to ignore these notices as just that many more pieces of unsolicited junk mail."[445] This hypothetical disregard by consumers also calls into question another argument set forth in defense of notification, which is the incentive provided for organizations to improve their information security practices. If consumers disregard the notification, organizations no longer fear reputational damage or potential loss of clients as a result of such notification.

The validity of arguments made both in favor of and against notification depends on empirical assessments of the influence of notification requirements on the incidence rate of identity theft. Sasha Romanosky *et al.* concluded how the adoption of data security breach notification initiatives demonstrates a marginal effect of just fewer than 2% on the rate of identity theft cases.[446] Despite this marginal effect, the authors emphasize the other benefits associated with data security breach initiatives, such as reducing the average victim's losses and improving an organization's security and operational practices. Other remarks made by Romanosky *et al.* refer to the obstacles faced to carry out their analysis.

---

[442] Lenard, T. M. & P. H. Rubin (2006). Much Ado about Notification. *Regulation*, Vol. 29 (1): 47.

[443] See for example Rode (2007: 1624) who states "[t]he successful protection against identity theft outweighs the associated costs."

[444] Garner, E.L. (2008). Is Comprehensive Federal Data Security Legislation Necessary to Protect U.S. Businesses, Consumers and the Government from Identity Theft and Other Crimes? Master Thesis Johns Hopkins University: 35.

[445] Oxley, M.G. (2005). Opening statement to the U.S. House Committee on Financial Services (2005). *Assessing data security: preventing breaches and protecting sensitive information*, Hearing, May 4, 2005 (Serial 109 – 23): 2.

[446] Romanosky, S., Telang, R. & A. Acquisti (2008). Do Data Security Breach Laws Reduce Identity Theft? *SSRN Working Paper Series*. Available at: http://www.ssrn.com.

These obstacles include the inability to obtain high-quality information on the incidence rate of identity theft from sources such as the financial service providers, a concern which others support.[447] The connection between data security breaches and actual incidents of identity theft remains an area of uncertainty, which also complicates the ability to measure the effectiveness of interventions such as data security breach notifications. The GAO aimed to determine the causal relationship between data security breaches and incidents of identity theft and concluded how "[c]omprehensive information on the outcomes of data breaches is not available. Several cases have been identified in which a data breach appears to have resulted in identity theft, but available data and information from law enforcement and industry association representatives indicated that most breaches have not resulted in detected incidents of identity theft."[448] More specifically, the GAO states how of the 24 large security breaches investigated only 4 turned out to have resulted in incidents of identity theft.[449]

ID Analytics, in turn, also conducted a study several years ago in 2007 and came to a number of key findings.[450] According to ID Analytics, smaller breaches maintain a higher rate of misuse than larger breaches. Moreover, the actual misuse of personal information ranged from one in 200 identities for breaches of fewer than 5,000 individuals to a misuse rate of less than one in 10,000 identities for breaches of more than 100,000 individuals. Those using the obtained personal information demonstrate a high rate of turnaround. Fraudsters generally used a single identity for no more than two weeks before moving on to the next identity.

Javelin Research & Strategy also published a report on the connection between identity theft and data security breaches. Hailed as "the first ever nationally representative report that shows the true known relationship between data breaches and actual occurrences of identity theft", Javelin described how only a small percentage of data breaches led to actual incidents of identity theft. Through its results, Javelin determined the publicity granted to the breaches to be counterproductive as such publicity misdirect consumers about the 'causes' of identity theft. Overall, James Van Dyke notes how "[g]overnments and corporations must ensure that their data breach 'cures' do not cause more problems than the breach."[451] Oddly enough, Javelin published another study several years later which concluded how " [i]f a consumer gets a data breach notification letter, they are four times more likely to suffer identity theft within the next year."[452] Perhaps there is a greater connection between data breaches and identity theft than Javelin desired to acknowledge previously. Javelin uses its results to demonstrate how notified consumers fail to take appropriate action to 'prevent and protect' themselves from identity theft. This conclusion seems

---

[447] See Hoofnagle, C. J. (2007). Identity Theft: Making the Known Unknowns Known. *Harvard Journal of Law and Technology*, Vol. 21: 98 – 122.
[448] GAO (2007b): 21.
[449] *Ibid.*
[450] ID Analytics (2007). Data Breach Harm Analysis from ID Analytics Uncovers New Patterns of Misuse Arising from Breaches of Identity Data: Pioneering Study Spans More Than a Dozen Data Breaches of Over Ten Million Identities. News Release. Available at: http://www.idanalytics.com/news-and-events/news-releases/2007/11-7-2007.php (last accessed October 9, 2010).
[451] Qtd. In 'Data Breaches Are Not the Leading Cause of Consumer Identity Fraud' (2006). Available at: http://markets.hpcwire.com/freelunch/news/read?GUID=212009 (last accessed July 13, 2010).
[452] Javelin Strategy & Research (2008). Consumer survey on data breach notification. Available at: http://www.tawpi.org/uploadDocs/Data_Breach_survey.pdf (last accessed July 12, 2010).

shortsighted since the options for consumers to protect themselves are limited and severely decreased *after* a data breach (see chapter 6).

3.4.2 The Netherlands

The introduction of a data security breach notification mechanism in the Netherlands came about mainly through the influence of developments in other countries, especially the United States, but also through developments at the European level. The first call for the introduction of a data security breach notification framework came in 2005 by representatives of the Socialist and the Labor Party. This call came during the evaluation process of the law on computer crime. The discussion as a result of this proposal for a data security breach notification initiative stranded as it never went beyond the stage of discussing arguments in favor of and against its introduction. The government parties, the Minister of Justice, along with the consumers union expressed views against the introduction of a notification requirement. The Minister of Justice believed self-regulation within the private sector proved sufficient.

Several years later, as officials at the European level already found themselves in the midst of a debate on the issue, the discussion also returned on the political agenda in the Netherlands. During the general meeting of the Lower House on the protection of vital infrastructures held on April 3, 2008, the Labor party proposed the idea of a notification requirement for large corporations.[453] Other events which stimulated the discussion and call for the introduction of a notification requirement include the airing of an episode of *Zembla*[454] in November 2008, where officials of the public prosecutor's office along with those from the DPA emphasized the need for such an initiative in the Netherlands. Through the airing of the episode, the issue began to receive more attention from the media and to a lesser extent from the public. On January 25, 2010, Bits of Freedom issued a position paper in favor of data security breach notification legislation.[455] The organization bases its position on the following points: the increase of storage of personal data in databases, the correlated increase of risks associated with potential leaks of such data, and the potential consequences of such data leaks for those involved. Therefore, those involved ought to have the right to be notified of such a leak. Bits of Freedom considers all parties to be responsible for notification when they suffer a leak. These notifications ought to go to the 'victims' as well as to an independent government agency.[456]

In order to develop a more comprehensive background on the topic, the Minister of the Interior promised the Lower House an exploratory study on the issue of data security breach notification mechanisms. Through an international quickscan, the study[457] provides a coherent and concise overview of the arguments made in favor of as well as in opposition to the introduction of a notification requirement. Especially the arguments listed against the notification requirement

---

[453] *Kamerstukken II* 2007 – 2008, 29 668 & 26 643, nr. 21.
[454] Zembla is a 'documentary' type television production.
[455] Bits of Freedom (BOF) (2010). *Position paper meldplicht datalekken*. Available at: https://www.bof.nl/live/wp-content/uploads/2010/01/datalekken-def.pdf (last accessed July 12, 2010).
[456] *Ibid.*
[457] Boer, L. & T. K. Grimmius (2009). *Melding Maken? Internationale quick scan meldplicht gegevens verlies*. Study commissioned by the Ministry of Economic Affairs.

deserve a brief moment of attention. Apparently, certain opponents use, or perhaps abuse, the financial crisis as an argument against the notification requirement. Since the financial crisis, according to these opponents, has already caused considerable damage to the trust consumers hold with regard to the financial sector, the introduction of a notification requirement shall only lead to a further decrease of trust in the sector. Closely related is the argument made against notification requirements by organizations who express the preference to keep information about the occurrence of a security breach indoors. This preference is in response to the fear of potential reputation damage. Both of these arguments focus on the potential damage such a notification can cause to the image of the company and the trust of consumers in such an organization.

As the researchers conclude, the notification requirement primarily appears to be used as a means to stimulate organizations to improve their information security practices, which hypothetically occurs due to the earlier mentioned fear of reputational damage. Furthermore, the researchers conclude, based on responses received from interviewees, how a notification requirement ought to apply to both the public and the private sector. But the interviewed experts noted how notification is not an appropriate instrument for consumers to reverse the potentially negative consequences of data loss.[458] In addition, the actual supervision and enforcement of such a notification framework is of crucial importance for the effectiveness of the requirement. Closely related, the researchers also emphasize how the supervisory organs or individuals must possess the necessary resources and liberty to carry out their mandate. Due to the availability of alternatives, there is not necessarily a need nor a desire for the introduction of a new separate organ to supervise and enforce the notification requirement. The researchers also conclude how respondents to their questions emphasized the favorable nature of harmonized European legislation with regard to notification requirements.

Other important features which surfaced as a result of the interviews conducted in the Netherlands are the need for a more comprehensive approach to the problem, which means that in addition to a notification requirement the government must also introduce other instruments or improve existing instruments. These include a fraud register much like CIFAS has in the United Kingdom, along with additional investigate capacity for the police with regard to hackers, and additional capacity for OPTA.[459] Other additional initiatives suggested by the respondents include the introduction of a whistle-blower policy or the obligation of an internal privacy officer for organizations.

The legislative development process in the Netherlands is strongly influenced by the anticipation of parallel developments at the European level. Ross Anderson *et al.* set forth a recommendation for the European Union to adopt a comprehensive security-breach notification law. Within their study, Anderson *et al.* aimed to determine which information security issues should be dealt with at the Member State level and which issues require the involvement of the European Union, either through harmonization or coordination. According to Anderson *et al.*, "[t]here has long been a shortage of hard data about information security failures, as many of the available statistics are not only poor but are collected by parties such as security vendors or law enforcement agencies that have a vested

---

[458] *Ibid.*

[459] OPTA is the Independent Postal and Telecommunications Authority.

interest in under- or over-reporting."[460] Furthermore, Anderson *et al.* describe how "[c]ompanies are hesitant to discuss their weaknesses with competitors even though a coordinated view of attacks could prompt faster mitigation to everyone's benefit."[461] Comprehensive security-breach notification could provide assistance with respect to this problem, according to Anderson *et al.* The authors refer to the situation in the United States, where security-breach notification has been an instrument since 2003.

The issue of notification after a breach had already been proposed in 2006 during the review of the EU regulatory framework for electronic communications networks and services.[462] Since the proposal was set forth within the specific context of Directive 2001/58/EC, its applicability proved limited to telecom and Internet Service Providers. As Anderson *et al.* note, the proposal "…would require notification to be made where a network security breach was responsible for the disclosure of personal data. This is a very narrow definition…and will only deal with a small fraction of cases that a California-style law would cover."[463]

The proposal for a notification requirement also received significant support from the European Data Protection Supervisor (EDPS). The EDPS believes that security-breach notification maintains various significant benefits. In its opinion, the EDPS writes how such notification "...reinforces the accountability of organizations, is a factor that drives companies to implement stringent security measures and it permits the identification of the most reliable technologies towards protecting information. Furthermore, it allows the affected individuals the opportunity to take steps to protect themselves from identify theft or other misuse of their personal information."[464]

Despite the general support for a comprehensive security-breach notification, political disagreements occurred between the various institutions. The main disagreement revolves around the actors the obligation ought to apply to. The EDPS along with the Article 29 Working Party members requested the notification requirement to apply to a wider range of actors, including online banks and other service providers. During its first reading, the European Parliament also supported such a broadening, but in the end the mandatory notification remained rather restrictive. A Directive was passed which inserted in Article 2(h) and 4(3) of the ePrivacy Directive "…a mandatory notification of personal data breaches by providers of electronic communications services and networks."[465] And claims, "[i]t is an important step towards enhanced security and privacy protection, although at this stage it remains limited to the electronic communications sector."[466] Furthermore, "[t]he Commission takes note of the will of the European Parliament that an obligation to notify personal data breaches

---

[460] Anderson *et al.* (2008): 3.
[461] *Ibid:* 18.
[462] European Commission (2007b). *Report on the outcome of the Review of the EU regulatory framework for electronic communications networks and services in accordance with Directive 2002/21/EC and Summary of the 2007 Reform Proposals.*
[463] Anderson *et al.* (2008): 24.
[464] European Data Protection Supervisor (2008). *Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*: C 181/3.
[465] European Commission (2009). Declaration on data breach notification. Annex to Directive 2009/136/EC.
[466] *Ibid.*

should not be limited to the electronic communications sector but also apply to entities such as providers of information society services. Such an approach would be fully aligned with the overall public policy goal of enhancing the protection of EU citizens' personal data, and their ability to take action in the event of such data being compromised."[467] This extension, however, remains to be seen.

The ultimate legislative proposal in the Netherlands incorporates two separate data security breach notification requirements.[468] The first concerns breaches of personal information. This notification requirement shall be hosted by OPTA. The second type of breach which requires notification concerns security and network integrity breaches. This type of notification is the responsibility of the Ministry of Economic Affairs. The legislative proposal envisions a single central point which receives both categories of notifications. This notification center is to function as a mailbox and as such is not to interfere or otherwise interact with the content of the complaints.[469] The notification center shall then forward the complaint to the responsible agency, which can be either the Ministry of Economic Affairs or OPTA, or both depending on the nature of the complaint.

On June 7, 2010, the DPA responded to the legislative proposal, which is a proposed amendment to the Telecommunications Act. In its response, the DPA stated how the introduction of a single notification center is not in line with the decision of the European Court of Justice which requires authorities with supervisory tasks to be able to carry out these tasks in an independent atmosphere.[470] The DPA envisions potential complications because of the intricate connection between breach of security and network integrity with the compromise of personal information. The detachment of both can also lead to inefficiency and unnecessary administrative burdens.

Other arguments or points of criticism raised against the legislative proposal are the restriction of the proposal to the telecommunications sector, whereas the DPA continues to advocate a broad notification requirement which includes all companies and government agencies. The DPA specifically refers to the usage of the instrument of notification as a means to prevent identity theft and as such describes how the restricted nature of the proposal therefore also restricts its effectiveness in that area. This is nearly the same criticism as raised at the European level, and is valid for the restriction to the telecommunication sector handicaps the potential effectiveness of the countermeasure.

3.5 Consumer Complaint Center

3.5.1 United States

When the Federal government criminalized identity theft in 1998, the government also introduced the mandate to introduce a consumer complaint center, which was to be stationed at the Federal Trade Commission. The data collected by the consumer complaint center was briefly discussed in chapter 1. The consumer complaint center serves a dual function through its accumulation of data on the

---

[467] *Ibid.*
[468] Memorie van Toelichting (2010). Consultation version, April 15, 2010. Available at: http://www.internetconsultatie.nl/nrfimplementatie/document/123 (last accessed July 13, 2010).
[469] *Ibid.*
[470] College Bescherming Persoonsgegevens (CBP) (2010a). Wetgevingsadvies CBP inzake wijziging van de Telecommunicatiewet.

prevalence and trends of identity theft next to its function as a source of information for (potential) victims of identity theft. Through both of these functions, the consumer complaint center aims to add to the body of knowledge and assist consumers in their efforts to resolve the problems associated with identity theft.

3.5.2 The Netherlands

The introduction of a consumer complaint center in the Netherlands as part of the public sector occurred in a vastly different manner in comparison to the United States. Discussions about the introduction of a consumer complaint center began in 2006, when a working group within the Ministry of Justice supported the idea. Actual implementation of the idea was seemingly pressed into the background, until a few years later in 2008 when the Ministry of the Interior and the Minister of Justice issued a joined press release about the introduction of a complaint center. This center was to be a pilot before a permanent center was to be introduced. This pilot complaint center commenced its activities in January 2009. Due to the lack of extensive human capacity, the existence of the complaint center was kept out of the spotlight. Even so, the pilot study managed to capture important information through a total of 241 complaints about identity theft or at least a suspicion thereof.[471] In the preface to the report of the study, it is stated how the consequences for victims of identity theft are significant. And that these victims are in dire need of government assistance in an effort to correct the errors which roam around various databases which have contaminated their good name. This assistance can most appropriately come from the central complaint center who must then also maintain sufficient power to ensure a level of effectiveness. For the complaint center is dependent on the other parties in the overall identification chain, namely law enforcement officials, municipalities, ministries, and others, to cooperate with the center to contain the problem of the victim to a minimum. Other relevant information obtained via the pilot study is the method used to conduct identity theft. Most complaints retraced the source of information used for the incident of identity theft back to open sources, whereas other main categories include phishing, hacking, or another type of cybercrime. The report fails to provide more details on its definition of open sources.[472]

In 2010, the pilot became a permanent complaint center. The government also installed a chain director, which is an official who receives the complaints and tries to contact partners in the identification chain to investigate the case.[473] When consumers first call the complaint center they reach Postbus 51.[474] This is to filter out the questions and only allow the more complicated cases to be transferred through to the chain director. The complaint center requires the consumers to have reported the incident to the police before they call the center.[475] After receiving the complaints, the chain director subsequently contacts chain partners in an effort to potentially investigate the case.

---

[471] Centraal Meldpunt Identiteitsfraude (2010). *Jaarrapportage 2009*.
[472] *Ibid.*
[473] Interview *Centraal Meldpunt Identiteitsfraude*, March 29, 2010, Amstelveen.
[474] Postbus 51 is Dutch government agency which serves as the central point of contact for citizens with questions addressed to the national government.
[475] Interview *Centraal Meldpunt Identiteitsfraude*, March 29, 2010, Amstelveen.

3.6 Cooperative Efforts

3.6.1 United States

On May 10, 2006, President George W. Bush issued Executive Order 13402 to 'strengthen federal efforts to protect against identity theft.'[476] Section 2 of the Executive Order established the Identity Theft Task Force,[477] which was to, among other things, "…prepare and submit in writing to the President within 180 days after the date of this order a coordinated strategic plan to further improve the effectiveness and efficiency of the Federal Government's activities in the areas of identity theft awareness, prevention, detection, and prosecution."[478] Nearly a year later, on April 11, 2007, the Task Force published its strategic plan. In its publication, the Task Force underscores the complexity of the crime, and the challenge identity theft presents to contemporary society. Through an overview of the problem, the Task Force focuses its strategic plan on improvements in four key areas. These include data protection, opportunity reduction, victim assistance, and deterrence.[479] With regard to the first key area identified, the Task Force introduces the following recommendations for data security in the public sector:

- Decrease the unnecessary use of Social Security Numbers in the public sector through the development of alternatives strategies for identity management;
- Educate federal agencies on how to protect data;
- Monitor their compliance with existing guidance;
- Ensure effective, risk-based responses to data breaches suffered by federal agencies.

For data security in the private sector, the Task Force recommends the establishment of national standards for private sector data protection requirements and breach notification requirements. Furthermore, the Task Force also recommends to better educate the private sector on data safeguarding practices and to initiate investigations of data security violations. Other recommendations include the introduction of a multi-year public awareness campaign by the private sector. Unlike for the public sector, the Task Force does not recommend a decrease in unnecessary use of SSNs in the private sector and instead recommends the development of a comprehensive record on private sector use of SSNs.

For the second key area, the reduction of opportunities, the Task Force recommends to hold workshops on authentication. These workshops are to engage academics, industry, entrepreneurs, and government experts on developing

---

[476] Executive Order 13402 - Strengthening Federal Efforts To Protect Against Identity Theft (2006).

[477] Members of the Task Force include: the Attorney General, who serves as Chairman of the Task Force, the Chairman of the Federal Trade Commission, who serves as Co-Chairman of the Task Force, the Secretary of the Treasury, the Secretary of Commerce, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, the Secretary of Homeland Security, the Director of the Office of Management and Budget, the Commissioner of Social Security, the Chairman of the Board of Governors of the Federal Reserve System, the Chairperson of the Board of Directors of the Federal Deposit Insurance Corporation, the Comptroller of the Currency, the Director of the Office of Thrift Supervision, the Chairman of the National Credit Union Administration Board, and the Postmaster General.

[478] Executive Order 13402 (2006): 3.

[479] Identity Theft Task Force (2007). *Combating Identity Theft: A Strategic Plan*: 4.

and promoting better ways to authenticate identities. The Task Force issues the recommendation in light of its belief in "[e]fforts to facilitate the development of better ways to authenticate consumers without burdening consumers or businesses—for example, multi-factor authentication or layered security—would go a long way toward preventing criminals from profiting from identity theft."[480]

Recommendations to improve victim assistance during their recovery of the crime include specialized training for first responders and others who offer direct assistance to victims of identity theft. More specifically, the Task Force recommends the government to train law enforcement officers, provide educational materials to first responders to use when approached by a victim, and develop and distribute an identity theft victim bill of rights. Moreover, the Task Force also recommends amendments to statutory law in order to ensure the monetary compensation of time spent on the recovery of the crime by the victim. The Task Force also recommends assessments on the efficacy of available tools for victims of identity theft, such as credit freeze initiatives along with the remedies offered through FACTA.

The last key area for improvement relates to the deterrence of future acts of identity theft through increased prosecution and punishment of offenders. Due to the increased sophistication of perpetrators of identity theft, the Task Force recommends the establishment of a National Identity Theft Law Enforcement Center. Other recommendations include enhanced information exchange between law enforcement agencies and the private sector along with the development of universal identity theft report form. With respect to coordination with foreign law enforcement, the Task Force recommends the United States to encourage other countries to adopt domestic legislation which specifically criminalizes identity theft. Just as the United States should encourage other countries to accede to the Council of Europe Convention on Cybercrime as a means to facilitate investigation and prosecution of perpetrators of identity theft. Finally, the Task Force also recommends increased prosecution of offenders of identity theft. To accomplish such an increase, the Task Force specifically recommends the designation of an identity theft coordinator for each United States Attorney's Office to develop a specific identity theft program for each district. Moreover, the Task Force recommends an evaluation of monetary thresholds for prosecution along with an encouragement of state prosecution of cases of identity theft. The Task Force also makes recommendations with respect to 'gaps' in criminal statutes. In particular, the Task Force lists the following aspects:

- Amend the identity theft and aggravated identity theft statutes to ensure that identity thieves who misappropriate information belonging to corporations and organizations can be prosecuted
- Add new crimes to the list of predicate offenses for aggravated identity theft offenses
- Amend the statute that criminalizes the theft of electronic data by eliminating the current requirement that the information must have been stolen through interstate communications
- Penalize creators and distributors of malicious spyware and keyloggers

[480] *Ibid:* 6.

- Amend the cyber-extortion statute to cover additional, alternate types of cyber-extortion.[481]

Overall, the Task Force states "…that all of the recommendations in this strategic plan—from these broad policy changes to the small steps—are necessary to wage a more effective fight against identity theft and reduce its incidence and damage. Some recommendations can be implemented relatively quickly; others will take time and the sustained cooperation of government entities and the private sector."[482]

In September 2008, the President's Task Force published a follow up report to assess the implementation of its previously produced strategic plan.[483] In its conclusion, the Task Force appears optimistic. "The efforts of the Task Force over the past year to implement the Plan's recommendations have underscored the need for a comprehensive and coordinated response from both the public and private sectors. These efforts have already made a difference and will continue to do so in the coming years."[484]

The concrete implementation of a recommendation set forth by the Task Force occurred through the introduction of the Identity Theft Enforcement and Restitution Act of 2008 (see section 3.1). This Act implemented the Task Force's recommendation to allow victims to receive compensation for their time needed to recover from actual or attempted acts of identity theft through criminal statutes.[485] Furthermore, "[t]hrough the Identity Theft Enforcement and Restitution Act of 2008 (Title II of P.L. 110-326), Congress, among other things, eliminated provisions in the U.S. Code requiring the illegal conduct to involve interstate or foreign communication, eliminated provisions requiring that damage to a victim's computer amass to $5,000, and expanded the definition of cyber-extortion."[486]

Selected other issues remain as of yet unaddressed, Finklea notes how, "Congress has not yet addressed the Task Force recommendation to expand the identity theft and aggravated identity theft statutes to apply to corporations and organizations as well as to individuals, nor has it addressed the recommendation to expand the list of predicate offenses for aggravated identity theft."[487]

3.6.2 The Netherlands

On May 15, 2008 the Ministry of Justice along with the Ministry of the Interior officially introduced the program *Versterking Identiteitsketen in de Publieke Sector* (VIPS), which is a program initiated to strengthen identification in the public sector. The program works on a combination of initiatives in an effort to prevent and counter identity theft along with identity mistakes in the public sector. Through an expert meeting held on November 4, 2009, the program formulated four goals.[488] These include:

---

[481] *Ibid:* 9.
[482] *Ibid.*
[483] Identity Theft Task Force (2008). The President's Identity Theft Task Force Report.
[484] *Ibid:* viii
[485] Finklea, K. M. (2010). *Identity Theft: Trends and Issues*. Congressional Research Service: 5.
[486] *Ibid:* 6.
[487] *Ibid.*
[488] Programma VIPS (2010). Programmaplan 2010 – medio 2011. Unpublished document.

1. Government agencies must improve their acknowledgement of risks and incidents of fraud and other mistakes in relation to identities, and they must respond in a better way. This requires better registration of incidents, but also an increased sense of urgency among government agencies, including investigation services. Furthermore, VIPS emphasizes the need for clarity about how to respond when incidents of identity theft occur.
2. Registrations and systems which maintain identification information must be reliable. The quality of data stored on source systems such as the *Gemeentelijke Basis Administratie* (GBA), or Municipal Personal Records Database can be improved along with the exchange of information between involved parties. Other areas of improvement include the information security of the systems in order to prevent attacks from outside. This can occur through the use of privacy enhancing technologies, where technology actually enables the improvement of information security rather than increase the risk of information exposure.
3. Victims must be able to resolve incidents of fraud or mistakes associated with their identities in a simpler manner. The government must support victims in their efforts to prevent and reverse mistakes with or incidents of fraud related to the victims' identities. Moreover, citizens must obtain more certainty that the government makes a sincere effort to prevent repeat victimization.
4. Citizens must become more aware of the risks of fraud and mistakes related to their identities and the actions which they can take to reduce the risks of such incidents.

These goals are listed according to the prioritization level of the goal, where logically the first goal maintains the highest level of priority. On December 1, 2009, the Steering Committee officially endorsed the goals as set forth by the expert meeting. Furthermore, the Steering Committee noted while the private sector currently falls outside of the scope of the program, businesses also maintain a viable role in the authentication and verification of individuals and their identities. As such a call for the private sector to become involved in the program's efforts seems appropriate according to the Steering Committee.

VIPS receives indirect support to accomplish its goals via other projects which aim to achieve similar results. To accomplish the various goals, VIPS supervises thirteen activities. For financial identity theft, the most relevant activities include:

1. Central Consumer Complaint Center
2. Tackling Abuse with Identification documents
3. Vision on Biometrics
4. Consultation of separate criminal offense for identity theft
5. Digital Identities
6. Fundamental research into the identification chain in the public sector

These goals and activities provide a comprehensive approach to the challenge of financial identity theft. Several activities are discussed elsewhere, such as the central consumer complaint center and the discussion about the introduction of a separate criminal provision for identity theft. The added value of VIPS therefore is

the anticipated ability of the program to coordinate and facilitate cooperation among the various public sector agencies engaged in the fight against financial identity theft.

3.7 Computer Emergency Response Teams

3.7.1 United States

The United States introduced its computer emergency response team in 2003 as the operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS). The DHS established NCSD to serve as the Federal government's cornerstone for cyber security coordination and preparedness, including implementation of the National Strategy to Secure Cyberspace. Within the National Strategy, the government remarks how "[i]n general, the private sector is best equipped and structured to respond to an evolving cyber threat. There are specific instances, however, where federal government response is most appropriate and justified."[489] The US-CERT called upon the experience and expertise developed by CERT CC, which has been around since 1988. Both of these organizations therefore work in close cooperation. The US-CERT "…is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with state and local government, industry and international partners."[490] In 2006, US-CERT began to issue quarterly trends and analysis reports to provide a summary and examination of the incident reports received by the organization. The US-CERT aimed to increase awareness about information security issues and to also reflect on emerging threats. Later on, these quarterly reports turned into monthly activity summaries, which the US-CERT publishes on its homepage.

In addition, US-CERT manages the National Cyber Alert System, which is the "…first cohesive national cyber security system for identifying, analyzing, and prioritizing emerging vulnerabilities and threats."[491] This system transmits computer security updates and warning information to all citizens, and as such provides everyone "…with free, timely, actionable information to better secure their computer systems."[492]

3.7.2 The Netherlands

The Ministry of the Interior introduced the Government Computer Emergency Response Team (GOVCERT) in 2002, after the publication of a study in two years earlier about the vulnerabilities of the Internet.[493] Its main objective is to support the government, including all levels of government, in the prevention and the treatment of ICT-related security incidents.[494] On a yearly basis, GOVCERT

---

[489] Department of Homeland Security (2003). *The National Strategy to Secure Cyberspace*: ix.

[490] United States Computer Emergency Readiness Team (n.d.). About Us. Available at: http://www.us-cert.gov/aboutus.html#events (last accessed July 12, 2010).

[491] United States Computer Emergency Readiness Team (n.d.). Frequently Asked Questions. Available at: http://www.us-cert.gov/faq.html (last accessed July 12, 2010).

[492] *Ibid.*

[493] Expert Meeting Cybercrime April 13, 2010, Maarsen, the Netherlands.

[494] The original introduction of a CERT in the Netherlands was CERT RO, which exclusively aimed to assist the national government. Soon the need and call for assistance at other levels of government

takes care of more than 150 incidents. To accomplish this objective, GOVCERT plays a vital role in the coordination through its position as central emergency point when an ICT-related security incident occurs. These include computer viruses, hacking, and the exploitation of other vulnerabilities in applications and software.

Furthermore, GOVCERT also serves as a source of information through its awareness materials and its yearly international symposium. In particular through the symposium, GOVCERT facilitates the exchange of information and knowledge which aims to benefit both the Dutch government and others across the world. Overall, GOVCERT plays a dual function within the role of the state as protector. The first is the protection offered by GOVCERT through its incident response system, and the second is GOVCERT's ability to deliver state of the art awareness about the most advanced type of threats. The latter function is especially crucial with respect to financial identity theft, since the realm of public policy needs such a source of information in an effort to determine how to respond to the problem.

3.8 Conclusion

This chapter distinguishes itself from the following chapters due to its focus on the means of protection exercised by the state to reduce or ideally prevent the facilitation and the occurrence of financial identity theft. Its placement is therefore perhaps slightly counterintuitive since much of what is discussed within this chapter returns in the remaining chapters, especially the relevancy of data protection and data security breach notification legislation along with the conclusions drawn by the Identity Theft Task Force and its Dutch counterpart. Even so, this chapter provides important insights into the response offered to the problem by the state as protector. Overall, the versatile nature of financial identity theft is reflected in the diversity of applicable instruments used by the state in its function as protector. This is also in part due to the connection between identity theft and other 'threats' to society, such as terrorism and money laundering.

To combat the problem, the government in the United States first turned to the area of criminal law which insufficiently covered identity theft as a criminal offense. The background to the introduction demonstrates the importance of policy entrepreneurs to build a strong case in favor of additional legislation. Simultaneously, the historical background of the United States within the area of criminal law also exposes the use, or perhaps abuse, of identity theft as a means to impact other issues of public policy, namely illegal immigration and terrorism. In this sense, identity theft is hijacked in order to serve other policy objectives. Or perhaps supporters merely try to kill two birds with one stone.

The government in the Netherlands distinguished itself from the United States through its alternative approach, but remains in anticipation of European developments which may lead to the implementation of a separate criminal offense after all. Interesting to note is how the government in the Netherlands plans to amend article 231 of the Criminal Code which concerns fraud with travel documents. In the letter which announces the anticipated amendment, the Ministry of Justice mentions look-a-like fraud, which is generally used by those

---

surfaced which allowed the CERT to transform into GOVCERT which provides its services to all agencies within the government, regardless of the level.

trying to gain illegal entry into the Netherlands. This amendment demonstrates the priority granted to look-a-like fraud and its connection to illegal immigration.

Despite the benefits for law enforcement officials and victims of identity theft, additional criminal legislation nevertheless maintains its limitations through the challenges which arise as a result of its enforcement. Financial identity theft, in particular when perpetrators conduct the crime via means of digital technology, is difficult to investigate and subsequently prosecute. Its investigation is also time and resource intensive. As Pontell and Geis note, "[t]he 'band aid, thumb-in-the-dyke' approaches that have characterized the American response to identity fraud are likely to embolden perpetrators who have an excellent chance to escape detection because of the limited capacity of enforcement agencies to respond to their crimes."[495] The deterrence aspect of criminal legislation also appears limited, especially with regard to perpetrators of financial identity theft, many of which must be keenly aware of the relatively low likelihood of being caught by law enforcement. As a means of protection, therefore, criminal law is limited. Even so, the incorporation of a situational crime prevention perspective in the Netherlands through the usage of experimental gardens in an effort to unravel and subsequently reduce the opportunity structure for cybercrime proves promising. For such an approach surpasses the traditional crime fighting objective of law enforcement.

Still, the criminal arena does not generally attend to the 'architecture of vulnerability' as Solove notes, when he writes "[t]he traditional legal view of identity theft fails to address this architecture, for it focuses on identity theft as a series of discrete instances of crime rather than as a larger problem about the way our personal information is handled."[496] Other sources also criticize the focus on criminal legislation as a means to combat identity theft.[497] Certain authors have therefore suggested the emphasis ought to be on prevention rather than detection.[498]

This leads to the importance of data protection and its connection to the facilitation of financial identity theft. The challenge of data protection increased through the use of computers as the historical backdrop in both the United States and the Netherlands illustrates. The difference in approach in both countries continues to be a topic of discussion, especially in light of arguments which favor the approach taken in the European Union. Even so, both the United States and the Netherlands are reaching out to other instruments such as data security breach notifications. The mere introduction of such a notification framework indicates the inability of current data protection regimes to safeguard personal information. This conclusion is strengthened through the emphasis placed on the use of such a notification system to provide incentives for the private sector to improve its information security practices. The introduction of data security breach notification proved to be inherently reactive to incidents which demonstrates how personal information is vulnerable to access by those with malicious intent.

---

[495] Pontell, H. N. & G. Geis (2007). 'New Times, New Crimes: "Blocking" Financial Identity Fraud' in F. Bovenkerk & M. Levi (eds.) *The Organized Crime Community*: *Essays in Honor of Alan A. Block*. New York: Springer: 54.

[496] Solove (2004): 115.

[497] See for example Matejkovic, J. E. & K. E. Lahey (2001). Identity Theft: no help for consumers. *Financial Services Review*, Vol. 10: 210-235.

[498] See for example Laylock, G. (2004). New Challenges for Law Enforcement. *European Journal on Criminal Policy and Research*, Vol. 10: 39 – 53.

The conclusions and recommendations of the Identity Theft Task Force and its Dutch counterpart strengthen the image of diversity and subsequent complexity of the problem. Both of these initiatives play a vital role in the development of a comprehensive framework of state action in response to identity theft. This precisely because they manage to take stock of the vulnerabilities and as such are in a position to issue and implement recommendations for improvement. The exposition of vulnerabilities is imperative to understand how the state as protector can reduce the facilitation of incidents of financial identity theft.

4 | State as Provider

Besides its function as protector of the people, the state also maintains a function as provider, at least since the early modern state (early 19th century). As provider, the state is responsible for the establishment of an identification infrastructure to serve as a framework for the provision of (social) services, but also to administer other aspects of daily life such as taxes, healthcare, education, employment of citizens, and others. Paul Schwartz captures the intricate connection between the service administration and its need for personal information.[499] As Schwartz writes, "[t]he state gathers information because distribution of social services is impossible without detailed information on the citizen as client, customer, or simply person to be controlled."[500] Moreover, the identification infrastructure established by the state also becomes the framework used in, for example, the financial services sector. This makes the identification infrastructure important for both the public and the private sector. This chapter provides an overview of the main components of the identification infrastructure in both the United States and the Netherlands. The main components include identification information, 'identification' numbers, identification documents, and instruments used for electronic identification or authentication.

4.1 Identification information

The accumulation of information, especially identification information, by the state is hardly new. As Colin Bennett notes, "[r]ecord keeping on individuals is as old as civilization itself. Historical research has traced the notion of a system of personal records back to most of the ancient civilizations of the Far and the Near East, Central and South America, and the Mediterranean. With few exceptions, however, such as William the Conqueror's renowned Domesday Book, the collection and keeping of personal records were localized and unsystematic."[501] Despite its historical origins, record keeping activities of states changed significantly several decades ago as technological advances developed innovative opportunities for the maintenance of personal records. Moreover, Bennett describes how an increase in information collected from and about citizens occurred due to an increase in the number and complexity of policies to be carried out by the state.[502] Simultaneously, the nature of the information collected for record keeping also experienced a transformation. Many of these changes, especially the technological advances, led to the introduction of information privacy or data protection initiatives as became evident in section 3.3. This section aims to shed a light on the actual information maintained by the state and its various agencies.

---

[499] Schwartz, P. (1992). Data Processing and Government Administration: The Failure of the American Legal Response to the Computer. *Hastings Law Journal*, Vol. 43: 1329.
[500] *Ibid:* 1332.
[501] Bennett, C. J. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithica, NY: Cornell University Press: 18.
[502] *Ibid.*

4.1.1 The United States

The information collected and maintained by the government in the United States both at the State and at the Federal level for administrative purposes is substantial. Michael Froomkin provides an overview of several illustrative types of federal government data.[503] These include Census data, Corporate Tax data, National Security Intercepts, Personal Tax Data, Military Records, Law Enforcement Data, Health Records (e.g. VA, Medical benefits programs), Passport Applications, Federal Employee Records, Immigration Records, Contracting/Purchasing, Regulatory Disclosures (e.g. trade secrets, required disclosures, results of inspections), Sealed court records, and Transfer program records (e.g. Social Security, Food Stamps, Veterans). In addition to the records maintained by the Federal government, State and local government agencies also maintain records. These include State tax data, State law enforcement data, K-12 & university educational records, State transfer program records, State court records, State regulatory data, records deposited in relation to Driver's License applications, State prison records, and records relating to foster children and other reports to child welfare agencies.[504]

Many of these records maintained include personal information[505] used for identification purposes which perpetrators desire to obtain to carry out the first stage of financial identity theft. The main examples include tax data, health records, passport applications, driver's license applications, and university educational records. As Froomkin notes, the government, both Federal and State, obtains such information mainly as a result of a legal mandate. As a result, citizens and other residents generally lack the right to veto such information accumulation. This is an essential observation since the record keeping activities of both Federal and State government agencies are in the spotlight as a result of numerous data breaches. Whereas Froomkin accurately notes how most attention is devoted to the breaches which occur in the private sector, the exceptional nature of the records maintained by the public sector also require extensive attention for its activities and (lack of) safeguards.

Froomkin observes how the public sector faces similar challenges as the private sector with respect to the vulnerabilities for data breaches. Even so, Froomkin argues "…while the public sector is vulnerable to all the risks that bedevil the private sector, there are some additional dangers that are either peculiar to the public sector or so different in scale as to amount to a difference in kind."[506] Various non-profit organizations have been active in the collection of information about data security breaches both in the public and the private sector. Such information accumulation demonstrates vital background information about the nature and the incidence rate of data security breaches. For the public sector, the Identity Theft Resource Center (ITRC) provides statistical information about

---

[503] Froomkin, A. M. (2009a). Government Data Breaches. *Berkeley Technology Law Journal*, Vol. 24: 1019 – 1060.

[504] *Ibid:* 1024.

[505] Froomkin (2009a: 1025) describes how personal data "…generally includes information that can be used to locate or identify an individual: name, address, telephone number, Social Security Number, driver's license number, account number, or credit or debit card number. It also includes more sensitive information, such as income, personal health records, military records, law enforcement investigatory records, and multifarious disclosures made in connection with the application for government licenses or benefits."

[506] *Ibid:* 1026.

the number of breaches and the number of records exposed as a result of such breaches. The ITRC bases its information on data security breaches which manage to capture the attention of the media. According to its report published in 2010, the government/military part of the report on data security breaches accounted for 18.1% of all breaches, but 35.6% of records were exposed as a result of such breaches.[507] The total number of records exposed was 79,470,963 within one year. Whereas certainly not all records are the result of intrusion by perpetrators of financial identity theft, these statistics do demonstrate the vulnerability of the information maintained by the state as provider and as such the potential for facilitation of the first stage of financial identity theft in the United States.

4.1.2 The Netherlands

In an effort to enhance the transparency of databases in the Netherlands, in the public as well as the private sector, the Data Protection Authority (DPA) commissioned a study to examine in how many databases the average citizen was registered.[508] The total provided in the conclusion of the study is 250 to 500 database registrations for the average citizen. For the public sector, Bart W. Schermer and Ton Wagemans note how the total number of databases during the last twenty years has grown tenfold. According to Schermer and Wagemans, the state is the most important processor of personal information in the Netherlands.[509] This occurs through a variety of databases, both general and sector specific.

The most pertinent database in the Netherlands is the Municipal Personal Records Database, or *Gemeentelijke Basis Administratie* (GBA). During the start of the eighties, the government introduced the GBA in response to a growing need to better synchronize information flows within the public sector in the Netherlands. The government deemed such synchronization necessary as a result of the proliferation of information systems. The development of the GBA also turned out to be a more acceptable alternative to the introduction of a central database of personal information, which the government originally desired.[510] Such a desire stumbled upon fierce resistance from a significant part of the Lower House.[511] Despite overlap between the original bill and its alternative, the government introduced a decentralized system through the GBA, which appeased the Lower House and still provided the government with the opportunity to develop a more efficient administration of information keeping. This efficiency came mainly through the automation of record keeping activities. Each municipality maintains its own GBA which includes information, such as name, address, marital status, date of birth, etc., about all individuals who reside in the municipality. Many different actors use the information maintained in the GBA. These include actors in both the public and the private sector.

---

[507] Identity Theft Resource Center (2010b). *2009 Data Breach Stats*. Available at: http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202009.pdf (last accessed July 4, 2010).

[508] Schermer, B.W. & T. Wagemans (2009). *Onze digitale schaduw. Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat*.

[509] *Ibid:* 15.

[510] *Kamerstukken II* 1984 – 1985, 18 600 VII, nr. 23.

[511] *Ibid.*

During the last decade, the GBA became a topic of considerable political and administrative attention. The government detected a need during the start of the millennium to obtain advice about whether and how the GBA needed to be modernized. To this end, the Minister of Large Cities and Integration Policy established the Committee Snellen in February 2000. The Committee needed to answer two central questions. The first question posed by the government concerned the possibilities for improvement of the GBA accessibility through the usage of modern ICT. The second question focused on how new technological developments could also be incorporated as a means to strengthen the position of the citizen in society and in particular with regard to the state.

In its findings, the Committee determined how an increase in mobility, a growing anonymity through various forms of electronic communication, and the scalability of ICT and web technology provided important influences which together developed a need for a modernization of the GBA. [512] Based on these influences, the Committee Snellen identified several objectives for the government. The GBA, according to the Committee, is to become the pivot of the identification infrastructure in the Netherlands in the near future.[513] The speed and the accessibility of the database must be increased, and the system must be available 24/7. This means municipalities and users of the GBA must introduce organizational and technical means to ensure direct access to the GBA. As a result, the usage of modern ICT is essential for the successful realization of this future role of the database. The Committee specifically refers to the application of web technology for such success.[514] The Committee also calls for a simplification of the GBA system, and deems such simplification essential due to the complexity of along with the extensive costs associated with the current system. This answers the first question posed by the government.

For the answer to the second question, the Committee calls for a more central position of the citizen.[515] To accomplish this objective, the Committee suggests a digital locker. Through the introduction of a digital locker, individual citizens obtain the ability to exercise more control over their personal information. The digital locker provides citizens the opportunity to access and request corrections of information maintained in the GBA and to control which agency or person receives information about them. The use of the digital locker is voluntary.

While the underlying idea of the digital locker, to make the government more transparent and grant citizens the opportunity to correct mistakes, receives positive feedback,[516] its actual implementation remains controversial. The terminology is misleading, according to Bert-Jaap Koops, because the Committee describes how the digital locker allows the citizens to become 'directors' of their personal information and its collection. Yet, the Committee overestimates the role of citizens in the overall idea of the digital locker. Citizens are still unable to decide what personal information the government collects. Furthermore, citizens are also not in a position to alter the personal information or to decide which government agencies can access the information. Instead, citizens can ask the government to

---

[512] Commissie Modernisering GBA (2001). *GBA in de toekomst. Gemeentelijke Basis Administratie persoonsgegevens als spil voor toekomstige identiteits-infratructuur.*
[513] *Ibid:* 7.
[514] *Ibid:* 8.
[515] *Ibid.*
[516] Koops, B. J. (2001). Een nieuwe GBA, digitale kluisjes en identificatiedrang. *Nederlands Juristenblad*, Vol. 32: 1555-1561.

correct mistakes in their personal information and they can decide which private parties have access to their personal information. These citizen 'rights' already exist. The digital locker serves merely as a facilitator to ease the manner through which citizens can exercise these rights.[517] To speak of citizens as directors therefore is misleading and to claim the digital locker is a means to strengthen the position of citizens in society is exaggerated, according to Koops.[518]

The recommendations set forth by the Committee Snellen became the foundation for the establishment of the program Modernization GBA. The government introduced the modernization program of the GBA in an effort to ensure the successful integration of the database as part of the broader electronic government movement. The modernization program officially started in 2004. Four years after the beginning, the government temporarily stopped the program. Problems surrounding the budget already caused alarming sounds in 2007 but the official stop occurred after problems began to arise about the objectives of the program, the realization of these objectives, and the costs associated with the program. The audit study determined how the business case developed for the program proved insufficient in terms of quality.[519] Additionally, the study also concluded how the business case played no part in the actual realization of the program. In particular the program governance did not match the result oriented character of the broad, complex, and risky project.[520] As a result, there was insufficient direction with respect to functionality, money, time, and risks as well as the responsibility associated with these aspects.

Despite the turbulent history and the negative feedback provided, the Modernization program of the GBA experienced a revival after the Deputy Secretary of the Interior received the results of various studies which aimed to determine the survivability of the program.[521] Around the same time, a Gateway Review was also conducted. The results of the studies and the Gateway Review together provided the foundation for the negotiations between the Ministry of the Interior, the Association of Dutch Municipalities, and the representatives of the 'customers' of the GBA which led to the revival of the program.[522] The revival turned out to offer the most benefits for all parties involved, based on the analysis provided by the studies and the Gateway Review. The modernization of the GBA is essential according to the national government as well as the individual municipalities and its financial savings outweigh the original costs of investment.[523] As a result, the Deputy Secretary signed an official agreement with the various stakeholders on March 5, 2009 to revive the program.[524]

The modernization of the program consists of various elements which demonstrate intricate connections with the overall electronic government movement. The modernization incorporates the call for 24/7 accessibility through the GBA-V. While the GBA is a decentralized system, the GBA-V adds a central touch to the organization. This central component is a virtual copy of all records

---

[517] *Ibid.*
[518] *Ibid.*
[519] Ministerie van Binnenlandse Zaken en KoninkrijksRelaties (2007). *Auditrapport. Audit Modernisering GBA.*
[520] *Ibid.*
[521] Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (2010). Brief aan de Tweede Kamer. Betreft Modernisering GBA, May 7, 2010.
[522] *Ibid.*
[523] *Ibid.*
[524] *Ibid.*

maintained in the 430 municipalities. This system is online and as such accessible 24/7. The GBA-V is already a reality and the next step is to develop GBA-V Full Service. This additional step shifts the responsibility for the system away from the individual municipalities and changes the oversight to a central system. Even so, the municipalities remain source owners and they also maintain the responsibility to keep the information up to date. After GBA-V Full Service, the government aims to realize GBA-V Modern Interfaces which allows for real-time information exchange between 'customers' and municipalities.

Other changes to the GBA include its official transformation into a source of basic registration information. As a basic registration source, the GBA became one of the so-called 'basic registries' which provide a unique source of essential and reliable information for all official bodies in the Netherlands. This demonstrates the increased importance of the GBA. After the legal changes made on April 1, 2007, the GBA officially became the exclusive provider of authentic personal information on citizens and residents in the Netherlands. This change enhances the significance of the integrity of the information maintained in the databases at all municipalities, especially since there is a legal obligation for all other agencies to retrieve their information from the GBA. Moreover, through the usage of the GBA, individuals only need to provide their information once. This one time information issuance on the side of the individual decreases the administrative burdens on the government and also makes the entire operation more efficient. The government also anticipates an increase in quality of the information since all administrative organs retrieve the reliable personal information from the GBA. Improved service delivery is another benefit which the government anticipates as a result of the onetime issuance idea.[525]

The increased importance of the GBA leads to potential problems with regard to the facilitation of the first stage of financial identity theft. First, the increased reliance on the GBA enhances its role as a single point of vulnerability. Since all organs return to the GBA as a unique source and anticipate a high level of reliability and accuracy, the integrity of the information must be high. Any mistake or alteration made in the system of information spreads all over the government's administration. This means that criminal entry into the system either through hacking or through normal registration provides perpetrators of financial identity theft with an important first step.

Since the integrity of the information in the GBA is of the utmost importance, the government has introduced a procedure for the information recipient to report back to the municipality. This must occur when the information recipient, or rather another administrative body, has reasonable doubt about the accuracy of the information. When the municipalities receive such a report about the accuracy of the information, they are under a legal mandate to investigate the report and to correct any mistakes in the information maintained in the database. When a 'customer' of the information either from the public or the private sector files a report, this must be done through the usage of the a-number or the citizen service number (see section 4.2.2) of the data subject. The report must subsequently indicate what part of the information is outdated, what the updated information is, and an explanation as to why this is the case, preferably with a reference to a 'source of information.' The report is received by an automated system which is to deliver the information to the municipality in question.

---

[525] *Kamerstukken II* 2005 – 2006, 30 514, nr. 3.

Problems, as previously noted, with the GBA can arise as a result of 'false' registration, where perpetrators of identity theft use false, falsified, or stolen source documents to gain entry into the system. Registration in the system subsequently provides the perpetrator with the ability to obtain other documents. In a quick scan of the identification infrastructure, such a problem is identified and categorized as high risk.[526] Such a classification is based on the fact that the GBA is the main source of identifying information for actors within and outside of the government. As a result, false information spreads like an oil stain. Other less urgent matters identified in the quick scan refer to the reliability of the information maintained in the GBA.[527]

The database itself, however, is also an attractive source for perpetrators due to its maintenance of personal information which is lucrative to obtain for financial identity theft operations. The digitalization of the database through GBA-V means an expansion of accessibility which in turn leads to an increased vulnerability. Access is no longer restricted to a particular place or time or to a particular municipality. As such the developments with respect to accessibility may lead to an increased risk of data compromise.

4.2 Identification Numbers

A close link exists between record-keeping practices and the issue of identification or administration numbers. This section provides a historical description of the developments which have taken place along the way to establish the current identification number systems in the United States and the Netherlands. The description is subsequently used to identify why and how the systems create or could create opportunities for perpetrators to take advantage of to commit financial identity theft.

4.2.1 United States

Introduced through the Social Security Act of 1935, the original goal and purpose of the social security number (SSN) was to function as a record keeping system. The SSN assisted the Social Security Administration to conveniently record work and retirement benefits of employees within the system. During the early years, individuals did not need to demonstrate any type of identification in order to obtain a SSN. Furthermore, Robert Ellis Smith notes how "[f]or many years, the 3-by-2 inch Social Security card bearing a person's number had the legend 'NOT FOR IDENTIFICATION' printed on its face."[528] Smith describes how many individuals interpreted this statement on the card as a means to prohibit the use of the number for purposes other than social security. He claims, however, that this was never the case. Instead, "[t]he purpose of the legend, the Social Security officials would say, was merely to notify anyone to whom a card might be presented that it should not be relied upon as evidence of identity."[529]

---

[526] Knopjes, F. & J. Loogman (2008). *Quick scan werking identiteitsinfrastructuur*. Programma Identiteitsmanagement: 19.
[527] *Ibid:* 21.
[528] Smith, R. E. (2000). *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*. Providence, RI: Privacy Journal: 288.
[529] *Ibid.*

During the presidency of Franklin D. Roosevelt, the SSN began to evolve and received a more prominent role in the identification infrastructure of the United States. Former President Roosevelt signed Executive Order 9397 in 1943 which required Federal agencies to use the SSN to identify individuals in any new 'system of accounts.' Roosevelt states in the Order how "...it is desirable in the interest of economy and orderly administration that the Federal Government move towards the use of a single, unduplicated numerical identification system of accounts and avoid the unnecessary establishment of additional systems."[530]

The system, as envisioned by Roosevelt, was in place for many years and the expansion continued when the United States Congress passed legislation which required banks and other financial service providers to obtain the SSNs of all clients, regardless of the production of taxable income.[531] The indirect consequences of the law, including the fact that a majority of banks decided to print SSNs on the checks of their clients, assisted in the growing availability of the number. Smith notes how "[o]ddly, while the Social Security number was becoming more and more a public piece of information...people in places of authority were treating it as an authenticator of a person's real identity, as if it were a secret identifier known only to the individual."[532]

The Secretary of Health, Education, and Welfare appointed an advisory committee in 1973 to investigate "the proliferating uses of numerical identifiers and the implications of personal databanks."[533] The advisory committee recommended against the adoption of a nationwide, standard, personal identification format.[534] The advisory committee furthermore recommended "...that use of the Social Security be limited to Federal Programs that have a specific Federal legislative mandate to use the SSN, and that new legislation be enacted to give an individual the right to refuse to disclose his SSN under all other circumstances. Furthermore, any organization or person required by Federal law to obtain and record the SSN of any individual for some Federal program purpose must be prohibited from making any other use or disclosure of that number without the individual's informed consent."[535]

This recommendation issued by the Advisory committee is based on its understanding of the potential dangers associated with excessive use of the number. More specifically, the Advisory committee indirectly refers to the threat of identity theft, when the committee writes, "[a]s long as the SSN of an individual can be easily obtained (some organizations list the SSNs of their employees or members in published rosters), both individuals and the organizations that use it as a password are vulnerable to whatever harm may result from impersonation."[536] This important warning influenced the establishment of partial restrictions on the usage of SSNs, such as written in the Privacy Act of 1974.[537] Even so, only a couple of years later in 1976, the United States Congress passed the Tax Reform

---

[530] Executive Order 9397 (1943). *Numbering System for Federal Accounts Relating to Individual Persons.*
[531] Smith (2000): 292
[532] *Ibid:* 92-293
[533] Health, Education, and Welfare Advisory Committee (1973). *Records, Computer, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems.*
[534] *Ibid.*
[535] *Ibid:* xxii.
[536] *Ibid:* 132.
[537] The Privacy Act of 1974 states "[i]t shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number."

Act Section 1211 of the Tax Reform Act, which provides agencies with the right to require individuals to provide their SSNs for identification purposes in the administration of various services.[538]

This section appears to contradict the previously initiated restrictions which granted individuals the right to refuse the release of their numbers. Moreover, Section 1211 also ignored the previously issued warnings by the Advisory committee about the potential risks and dangers associated with the extensive usage of SSNs, especially for identification purposes. This proved to be merely the tip of the iceberg, as throughout the subsequent decades the SSN evolved into a general identification number, for both the public as well as the private sector. As the Government Accountability Office (GAO) notes, "[w]e found that information resellers, CRAs, and some health care organizations routinely obtain SSNs from their business clients and individual customers and have come to rely on SSNs as identifiers that help them verify an individual's identity and accumulate information about that person."[539] The GAO reached a similar conclusion several years earlier as well.[540] The evolution of the usage and availability of the SSN came accompanied by many warnings from the start as the report issued by the Advisory committee illustrates.

During the start of the nineties, the United States Congress held a hearing which exposed the existing problems with the availability and usage of the SSN through expert testimony.[541] Gwendolyn S. King, Commissioner of Social Security, U.S. Department of Health and Human Services, expressed her concern about the potential harm associated with exposure for individuals.[542] Smith noted during his testimony how the proliferating usage of the SSN in both the public and the private sector mainly occurred as a result of laziness.[543] Jeffrey Rothfreder in turn connects his statements directly to the problem of financial identity theft when he states how "[q]uietly, people with checkered motives are turning easy access to social security numbers into an epidemic of financial scams, invasions of privacy, and unregulated mischief. And it's only getting worse."[544] The continuous

---

[538] Social Security Act. 42 U.S.C. 405(c)(2)(C)(i) states "[i]t is the policy of the United States that any State (or political subdivision thereof) may, in the administration of any tax, general public assistance, driver's license, or motor vehicle registration law within its jurisdiction, utilize the social security account numbers issued by the [HEW] Secretary for the purpose of establishing the identification of individuals affected by such law, and may require any individual who is or appears to be so affected to furnish to such State (or political subdivision thereof) or any agency thereof having administrative responsibility for the law involved, the social security account number (or numbers, if he has more than one such number) issued to him by the Secretary."

[539] Government Accountability Office (2004b). *Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information.* GAO-04-11.

[540] General Accounting Offce (1999a). *Government and Commercial Use of the Number is Widespread.* GAO-HEHS-99-28.

[541] King, G. S. (1991). Statement to the U.S. House Subcommittee on Social Security of the Committee on Ways and Means. *Use of Social Security Number as a National Identifier.* Hearing, February 27, 1991 (Serial 102 -11). She furthermore states during her testimony how "…the majority of the social security number records today, over 60 percent, still are based on the assertions a person made at the time he or she applied for a Social Security Number. That, of course, means that the Social Security Number simply cannot be used effectively as a means of identification. And yet today it is widely used for non-Social Security purposes in the both the public and the private sectors. This expanded use was hastened by the computer revolution in the 1960s which combined with the simplicity of using a unique number that most people had already been issued, provided the major impetus for widespread use of Social Security numbers."

[542] *Ibid:* 20.

[543] *Ibid:* 48.

[544] *Ibid:* 74.

attention devoted to the facilitation of financial identity theft certainly demonstrates the escalating character of the problem. Furthermore, the GAO stated in 2004 how the organization previously testified before the Subcommittee on Social Security, House Committee on Ways and Means about the problems associated with the Social Security Administration enumeration and verification processes along with the potential consequences of the aggregation of personal information, such as SSNs, in large corporate databases. Moreover, the GAO also emphasizes the potential problems associated with the public display of SSNs in various public records and how all of these aspects could lead to opportunities for perpetrators of financial identity theft.[545] Others also anticipated and emphasized the same problem.[546]

Through the recommendations set forth by the Identity Theft Task Force (see section 3.6.1), the problems associated with SSNs finally receive more attention. Part of the Strategic Plan issued by the Identity Theft Task Force called upon the Federal Trade Commission (FTC), among other agencies, to examine the usage of SSNs by the private sector. Moreover, the Task Force also desired to develop a deeper understanding of the connection between SSNs and identity theft. Based on this information, the Task Force Strategic Plan requested the agencies, especially the FTC, to propose approaches which maintained the beneficial usage of the SSN in contemporary society but also decrease its availability and value to perpetrators of identity theft.[547] Through a cooperative effort with other Task Force agencies, the FTC issued a report in 2008 which listed five specific recommendations focused on private sector usage of the SSN.[548] These recommendations include:

- Improve consumer authentication;
- Restrict the public display and the transmission of SSNs;
- Establish national standards for data protection and breach notification;
- Conduct outreach to businesses and consumers; and
- Promote coordination and information sharing on use of SSNs.

In its report, the FTC reemphasizes the pivotal connection between SSNs and identity theft. The FTC recognizes how SSNs are often viewed as the "keys to the kingdom." The improved consumer authentication recommendation primarily targets the need to increase the effort to use SSNs as an instrument or tool to commit identity theft. The restriction on public displays and transmissions, on the other hand, aims to decrease the availability of the number in an effort to increase the difficulty of obtaining SSNs.

Despite the general consensus about the problematic association between SSN availability and usage, Fred H. Cate disagrees. He states how "[u]biquitous Social Security Numbers help identify people and ensure that information is associated

---

[545] Government Accountability Office (2004b): 6

[546] See for example Rotenberg, M. (1991). The Use of the Social Security Number as a National Identifier. *Computers & Society*, 21 (2-4): 13-19. Berghel, H. (2000). Identity Theft, Social Security Numbers, and the Web. *Communications of the ACM*, Vol. 43 (2); Solove, D. J. (2003). Identity Theft and the Architecture of Vulnerability. *Hastings Law Journal*, Vol. 54: 1227 – 1276.

[547] Federal Trade Commission (2008). *Security in Numbers: SSNs and ID Theft*.

[548] *Ibid.*

with the correct person. These two critical roles are essential to many valuable activities from facilitating national competition to locating heirs and missing children to enhancing national security. Accessible Social Security Numbers are also critical to preventing, detecting, and remedying identity theft, yet they appear to play little if any role in contributing to most cases of identity theft."[549] Cate rejects the connection between the facilitation of financial identity theft and the usage of Social Security Numbers. But the statements provided against such a rejection come accompanied by various other sources which negate the validity of his argument.[550] He appears to be relatively lonely in his assertions and as such his arguments pale in comparison to the opposing evidence.

The availability problem of the SSN became exacerbated when Alessandro Acquisti and Ralph Gross developed an algorithm to predict existing numbers based on information such as place and date of birth. As the authors note, "[t]he predictability of SSNs is an unexpected consequence of the interaction between multiple data sources, trends in information exposure, and antifraud policy initiatives with unintended effects."[551] This demonstrates how the changes made to the system in an effort to reduce the facilitation of financial identity theft through SSNs must focus on the usage rather than the availability, for the latter can no longer be contained by changes in policies due to the predictability of the number.

4.2.2 The Netherlands

The usage of personalized numbers as a tool in government administration in the Netherlands maintains a diverse background. The ability to issue general administration numbers to individuals by municipalities who desired to automate their population administrations started in 1967 through the *Rijks Computer Centrum* (RCC).[552] After the Committee Westerhout set forth its recommendation in 1970, the introduction of a uniform administration number in the Netherlands gained momentum.[553] The main argument in favor of such a number was the ability to efficiently store, process, and subsequently find personal information about citizens in the Netherlands. This proved particularly lucrative due to the introduction of automated systems. During the installation of the Committee, the Assistant Secretary of the Ministry of the Interior specifically speaks of an administration number which excludes identifying information such as date of birth, gender, or part of the name of the person.[554] This choice for a 'random'

---

[549] Cate, F. H. (2004). Testimony to the U.S. House Subcommittee on Social Security of the Committee Ways and Means. *Enhancing Social Security Number Privacy*, Hearing, June 15, 2004 (Serial 108-59): 7.

[550] In response to questions sent by Chairman Clay Shaw of the Subcommittee on Social Security of the Committee on Ways and Means, Chris Jay Hoofnagle and Ed Mierzwinski described how "[w]e strongly disagree with the proposition advanced by Mr. Cate in oral and written testimony on June 15, 2004 that the Social Security Number (SSN) does not play a major role in identity theft. Common sense, the experience of identity theft clearinghouses, identity theft litigation, and the academic literature support the proposition that the SSN plays a primary role in identity theft. It is almost impossible to obtain credit without a SSN, making possession of the identifier a necessary condition for the commission of identity theft."

[551] Acquisti, A. & R. Gross (2009). Predicting Social Security numbers from public data. *Proceedings of the National Academy of Sciences of the United States of America (PNAS)*: 10980.

[552] *Kamerstukken II* 1984-1985, 18 383, nr. 2.

[553] Commissie Westerhout (1970). *Rapport inzake registratie van persoonsgegevens*. Staatsuitgeverij 's-Gravenhage.

[554] *Ibid:* 46.

number as opposed to an 'identification' number is in part based on the recommendations set forth by the Committee Simons.[555]

The government planted the seed for the introduction of the administration number, or a-number, in 1971. According to Frank Kuitenbrouwer, its introduction was done in a rather secretive manner without too much commotion, through an amendment to a royal agreement.[556] This could mainly be accomplished due to the fact that such an amendment does not require the approval of the Lower House. The secrecy surrounding the introduction must have been the result of the sensitive nature associated with attaching numbers to people by governments. Several years later, in 1985, the discussion about the usage of administration numbers within the government continued. The Deputy Secretary of the Ministry of the Interior provided the Lower House with a memorandum which provided a depiction of the situation with respect to the usage of administration numbers at that time.[557] In the memorandum, the Deputy Secretary describes how several numbers exist within various systems since nearly each agency uses a special number. This is understandable, according to the Deputy Secretary, since each agency aims to meet its own specific needs. The usage of a general administration number as introduced in the bill for a central population administration receives little attention from individual agencies. As a result, the actual exchange of information between agencies still occurs manually, according to the Deputy Secretary, and through the usage of rudimentary identifying information such as name, address, and place of residence.[558] Agencies must use this information due to the lack of a general administration number. Since the numbers used by various agencies are incompatible, they need to use additional information. Such usage of additional information is undesirable and the Deputy Secretary therefore aims to demonstrate the attractive nature of a general administration number for information exchange among and between the various government agencies. The introduction of a general administration number leads to internal efficiency and improved performance, according to the Deputy Secretary. Moreover, such a number also assists in the prevention of mistakes, which is important for citizens.

Parallel to the developments of the a-number, the government also began to discuss changes to other numeric systems. The tax administration agency in the Netherlands had been using a *landelijk vast nummer* for many years for its internal administration. Among other things, the number was listed on individual tax return forms issued by the agency. During the early eighties, the government informed the Lower House about its plans to extend the usage of the number to employers.[559] These plans proved a response to the publication of a report by an interdepartmental steering committee which focused on illegal use of government benefits. The Deputy Secretary emphasizes the focus on limited use of the number and the continued separation between the usage of the tax administration number and the introduction of a general administration number.

---

[555] Commissie Simons (1968). *Rapport inzake verstrekking van inlichtingen uit de bevolkingsregisters*. Staatsuitgeverij 's-Gravenhage.
[556] Kuitenbrouwer, F. (1991). *Het recht om met rust gelaten te worden*. Amsterdam: Uitgeverij Balans: 79 – 80.
[557] *Kamerstukken II* 1984 – 1985, 18 383, nr. 2.
[558] *Ibid.*
[559] *Ibid.*

On January 7, 1983, the government officially launched its plan to implement a fiscal number by January 1, 1986.[560] Simultaneously, the government also expressed a desire to introduce a social security card in an effort to combat and reduce abuse of social security services. Through discussions between the government and the Lower House, the focus shifted away from a card and onto a number, a 'social' number. This number was to have close ties to the fiscal number. The actual introduction of a combined or social-fiscal number was an issue which the government originally hesitated on due to the ambiguity about the potential for privacy invasive aspects of such a plan.[561] Such a social-fiscal number proved a source of reluctance for the government, since a social-fiscal number would be a uniform number for the tax and the social security administrations. The scalability of such a number certainly seemed an important consideration for the government during its decision making process. Even so, the government proved determined to venture upon a reluctant path and aimed to introduce sufficient safeguards to ensure the privacy of its citizens. This transformation from reluctance to determination mainly came as a result of the report published by the interdepartmental steering committee which identified the promising potential of a combined number as an instrument to combat fraud.[562]

The introduction of a social-fiscal number seemed, according to the Deputy Secretary, an apparent and logical development due to an intricate connection between the tax and the social security administrations. The added benefit of revenue as a result of better information processing practices through the usage of the social-fiscal number certainly provided another positive stimulation for the developments and its speedy implementation.[563] Nevertheless, such a number was still not to be equated with a general administration number since its usage was to remain restricted to the areas of taxation and social security.

During the discussions on the proposal of an introduction of the social-fiscal number, several members of the Lower House issued a motion to unify the social-fiscal number and the a-number. This seemed like a logical development, as expressed in the parliamentary motion. In its response, the government rejected the plans to unify both numbers.[564] The government based its rejection on a variety of reasons. Perhaps the most relevant to mention here are the limits set on the usage of both numbers. The a-number is restricted to the public and the semi-public sector. The Lower House specifically participated in the development of these usage boundaries restricted to the public and the semi-public sector. The social-fiscal number, in contrast, must be available to the private sector due to the legal requirement for employers to use the number in communication with the tax administration. This conflict between the boundaries of the usage of the number is a major obstacle against integration of both the a-number and the social-fiscal number. Moreover, as noted on various occasions, it is not the intent or objective of the social-fiscal number to function as a general administration number. This is after all why the government introduced its plans to develop an administration number.

On January 1, 1989 the government officially introduced the social-fiscal number. The original objective of the number was to serve the needs of executive

---

560 *Ibid.*
561 *Ibid.*
562 Kuitenbrouwer (1991): 88.
563 *Ibid:* 89.
564 *Kamerstukken II* 1988 – 1989, 21 178, nr. 1.

agencies in the area of taxes and social security. Shortly after the introduction, the government agreed to include the number as part of the municipal social services administrations. Such inclusion proved desirable due to, among other reasons, the verification of personal information provided.[565] The government eventually extended the usage and circulation of the number to include all municipalities. And in 1994, the government officially agreed to the inclusion of the social-fiscal number in the Municipal Personal Records Database. Among the primary benefits of the inclusion was the ability of social security and fiscal agencies to request personal data maintained in the Municipal Personal Records Database. To request such personal information, these agencies managed to use the social-fiscal number as an 'access key.'

The expansion of relevant actors within the social-fiscal circuit demonstrates the erosion of original restrictions. As a matter of fact, the continuous resistance demonstrated by the government against the conversion of the social-fiscal number into a general administration number proved severely weakened by the ultimate outcome of the situation. For in 2002, the Interdepartmental Committee van Thijn determined how part of the problem was the existence of multiple numbers, including the a-number, social-fiscal number, and specific sectoral numbers, which were part of a policy framework dating back to 1994 that received little compliance.[566] The Interdepartmental Committee describes the original intent of both the a-number and the social-fiscal number. For the former was to evolve into a general administrative number used across agencies within the public sector, whereas the latter was to remain restricted to the field of social security. In practice, as the Interdepartmental Committee notes, the social-fiscal number evolved into a general number since it was used on a broad scale. The a-number, in contrast, remained secluded through its exclusive usage within the Municipal Personal Records Database. This reality, according to the Committee, led to considerable questions about the issue of numeric systems in contemporary Dutch society and especially the aspect of privacy.

The identification of problems in the system leads the Committee to the introduction of an alternative plan. The Interdepartmental Committee van Thijn introduces the idea of a citizen service number. This number is to be empty in terms of identifying information and the number must be known to its holder. When the government requires a number during communication with its citizens, they can provide the citizen service number. The actual citizen service number is to remain identical to the social-fiscal number. The citizen service number differs from its predecessor in other respects. For the citizen service number is different in terms of its maintenance, legal basis, and usage. The responsibility for the maintenance of the number rests with the individual municipalities through the Municipal Personal Records Database. Every information exchange must contain an explicit legal basis which affirms the usage of the citizen service number in a specific situation. The usage, according to the Committee, ought to be divided into three separate categories, namely organizational, sectoral, and national.[567] Each user category shall maintain specific arrangements. Every minister must introduce a specific sector number which can be the equivalent of the citizen service number as long as the Ministry maintains arrangements which implement

[565] Sociaal Economische Raad (1990). *Invoering sofi-nummer.* Advies 90/06.
[566] Tafel van Thijn (2002). *Persoonsnummerbeleid in het kader van identiteitsmanagement.*
[567] *Ibid.*

privacy enhancing technologies. When a Ministry or government agency is responsible for the treatment of special information, as identified by the Dutch Data Protection Act, the number used shall in principle not be the equivalent of the citizen service number. To ensure careful usage, the Committee also details a recommendation which introduces the notion of 'trust functions.'[568] These trust functions maintain a responsibility for the arrangements of authorization, authentication, and integrity at three different levels, namely the previously identified categories.

With respect to the private sector, the Committee specifically states how organizations within such a sector ought to only be allowed to use the number in service of a public task or when there is a legal requirement for the usage of the number during communication with the government.[569] An example of such a requirement is the need for employers to use the number when communicating employee information to the tax administration agency.

As its final recommendation, the Committee makes a crucial distinction when it states how the citizen service number should indicate who someone is rather than what the individual in question is entitled to in terms of services. The Committee emphasizes the need for practical measures to prevent the citizen service number from evolving into a pseudo identity.[570]

The plans as introduced by the Committee along with the observations made are particularly puzzling with respect to the background sketched above. For the continuous resistance demonstrated by the government to prevent the social-fiscal number from evolving into a general number used for all governmental and business communications failed to materialize, just as its original plan did for the a-number. As a result, the implementation in practice managed to accomplish precisely what members of the Lower House failed to successfully achieve several years ago. The only exception is that integration never occurred since the a-number continues to exist in its secluded form.

The background to the plan as published by the Committee also found its inspiration from experiences abroad. For the members of the Interdepartmental Committee visited Sweden to observe a country which carries many years of experience with a general identification number system.[571] In contrast to the United States, the Swedes and their experiences proved more positive. Still, abuse of access to personal identity numbers and other aspects of personal data do happen. Lars Regenfeldt from the National Tax Board recognizes how there are approximately 20 to 30 cases a year.[572] Yet the abuse of identifying information or the access to such information is not a reason for the population or the government to question the effectiveness and the advantages of the use of a personal identity number. Other government officials demonstrate similar views. When asked about the tremendous risk of fraud as a result of a unique identification number, they did not view this as a problem. There is fraud in Sweden, as anywhere else, but, according to representatives from the National Social Insurance Board, this has rather little to do with the existence and usage of the personal identity number. Despite the fact that the number is extremely available, fraud is difficult to commit when a perpetrator only possesses the

---

[568] *Ibid.*
[569] *Ibid.*
[570] *Ibid.*
[571] See appendix of *Ibid.*
[572] *Ibid.*

personal identity number of a potential victim. A perpetrator simply needs a lot more personal data to commit any type of identity-related crime. Fraud is hard work in Sweden, according to the National Social Insurance Board representatives. Yet, despite these comforting conclusions, restrictions have been introduced, especially within the private sector. Health insurance agencies are no longer allowed to use the number within their internal client administration.

The plan published by the Interdepartmental Committee van Thijn served as the basis for the proposal introduced by the government for a citizen service number. The introduction of such a number formed an important pillar of an overall program introduced which aimed to establish a 'different government.'[573] The legal framework for the citizen service number grants all government agencies the right to use the number without the need for additional legislative permission. The usage of a single number for government operations therefore stimulates efficiency and a reduction of administrative burdens. The introduction of the citizen service number allowed the government to streamline its information systems and also introduce the necessary conditions for efficient information exchange between the various government agencies. Furthermore, the introduction of the citizen service number also intended to engage in a major clean up of the previous social-fiscal number system. This clean up was necessary due to the existence of duplicate numbers along with abuse of social-fiscal numbers by individuals in an effort to work legally in the Netherlands despite their illegal immigration status or to receive government benefits which individuals were not entitled to.

The government specifically focused on introducing a citizen service number for public sector usage and states how the usage of the number within the private sector is of a different nature.[574] As a result, such usage is not discussed by the government during its presentation of the proposal. This ambiguity led to critical questions from the Lower House.[575] As a result, the Ministry of the Interior aimed to generate more clarity about private sector usage of the social-fiscal number in an effort to make decisions about the connection between the citizen service number and potential private sector usage.[576] This desire led to a study which evaluated usage of the number by semi-public and private parties. The study notes how the Dutch Data Protection Act requires a legal foundation in order for an organization to use a personalized number. Despite this legal mandate, many occasions demonstrate how the number is requested or used without any foundation. This includes illegal use by information agencies (see chapter 7) in an effort to more easily obtain certain kinds of personal information for a client and illegal usage of the number by illegal immigrants to work legally in the Netherlands.

Besides these obvious illegal situations, other organizations also use the number as an index mechanism or a search function.[577] In their report, the authors carefully conclude how there appears to be a general perception within the private

---

[573] Actieprogramma Andere Overheid (2003).
[574] Memorie van Toelichting voorstel van Wet BSN (2007). Unofficial version. Available at: http://www.bprbzk.nl/BSN/Informatiebank/Juridisch (last accessed July 4, 2010).
[575] TILT (2007). *Het gebruik van het sofinummer door private en semi-publieke partijen: feitelijke trends in gebruik en normering.* Interne notitie ten behoeve van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.
[576] *Ibid.*
[577] *Ibid.*

and the semi-public sector that possession of the number in their databases also provides them with the legitimacy to broadly use this number, or that such usage ought to be legitimized.[578] Overall, the study demonstrates how the number is susceptible to potential function creep, although not to the extent as became evident in the United States.

For the citizen service number, the government aims to limit such function creep through describing how the number serves as a means to indicate who someone is as opposed to what the individual is entitled to. The number itself does not grant individuals the right to certain services or privileges which means the mere possession is meaningless, according to the government. This is a position which reflects the statements made by the Interdepartmental Committee van Thijn.

Even so, criticism against the introduction of the citizen service number proved fierce. The DPA presented ten objections to the government's original proposal.[579] According to the DPA, the introduction of the citizen service number served primarily as a beneficial tool for the government, while the risks for citizens were insufficiently acknowledged. The DPA declared how it is too easy to assume that government efficiency is always in the interest of the citizens and that therefore the introduction of a general registration number is essential to the public. After all, the DPA reasoned, citizens can experience significant disadvantages as a result of the ease with which others, especially those with malicious intent, can access sensitive personal information. The DPA demanded government imposed requirements for the security of ICT systems which maintain citizen service numbers and related information.[580]

Another objection introduced by the DPA was the danger of the spread of mistakes through the use of the citizen service number. When incorrect personal information enters the computer or when incorrect processing occurs, citizens can experience significant harm as a result of such incorrect information.[581] This can happen in particular through the exchange of personal information based on the citizen service number. The correction of such mistakes poses additional challenges for citizens due to the lack of an office where they can request a correction. The government responded to this criticism through introducing a complaint center where citizens can go when they experience problems with their citizen service number. The original proposal also failed to adequately arrange situations where government agencies discover mistakes and need to notify the citizen. But this criticism also received a response from the government through a legal notification duty.

The most relevant objection posed by the DPA is the potential increase in identity theft as a result of the citizen service number. The DPA demonstrates little doubt about such a possibility and refers to experiences abroad. Illegal use of social-fiscal numbers is already a material fact which allows the DPA to develop an argument where such illegal use will suffer an increase due to the broader application of the citizen service number.[582] The consequences for citizens will

---

[578] *Ibid:* 3.
[579] College Bescherming Persoonsgegevens (CBP). (2005a). Advies wetsvoorstel algemene bepalingen burgerservicenummer.
[580] *Ibid.*
[581] *Ibid.*
[582] *Ibid.*

also be more severe due to the broader application, but the government's proposal fails to take this concern into account.[583]

The citizen service number proposal also received criticism from the academic arena.[584] Especially its misleading title, citizen *service* number, proved a source of criticism. This criticism stems from the understanding that the citizen service number predominantly serves the government through its ability to eliminate administrative burdens.[585] The notion of the government to combat identity theft through the incorporation of the number also receives objections, in particular since the introduction of the number also has the ability to lead to a more vulnerable identification infrastructure in the Netherlands, as the DPA noted as well.

During the oral discussion of the bill in the Senate, the government also received several objections and concerns.[586] The Senate appeared in particular concerned about the government's implementation of the number and the alternatives offered to citizens when mistakes occur. In addition, the Senate expressed its dissatisfaction about the fact that many agencies, predominantly in the health care sector, already used the term citizen service number, despite the lack of approval granted by the Senate to pass the bill into law. Whereas the majority of comments provided by various members of the Senate focused on the implementation of the citizen service number, along with opportunities for citizens to correct errors made on their behalf due to the usage of the number, at least one member referred back to the potential for identity theft as a result of the introduction and usage of the citizen service number.[587] While the government projected the introduction of the citizen service number as a means to reduce fraud, others appear to believe the number and its usage can provide opportunities for perpetrators to commit identity theft. The representative for the Green Party acknowledged how identity theft cannot be prevented or entirely avoided, to which the Assistant Secretary of the Ministry of the Interior logically responded: "but you can improve the situation."[588] The subsequent comment provided by the representative of the Christian Democratic Party, on the other hand, appears rather peculiar. He states, "[t]here are of course all different kinds of ways to commit identity theft. The number of methods to commit identity theft continues to expand and to some extent this is a good thing, because it shows that people are intelligent. They continue to think of something new. We can, in turn, also think of something new to prevent fraud. That's how we keep each other busy, and that is good."[589]

The State appears to set forth an argument which focuses on the impossibility of the complete prevention of identity theft in particular and fraud in general. Simultaneously, the State claims how it maximizes its efforts to reduce the potential for fraud. Through a study about the 'good' use of the citizen service number, *Het Expertise Centrum* (HEC), or the Expert Centre, re-emphasizes this notion.[590] HEC identifies the potential for identity theft through the introduction

---

[583] *Ibid.*
[584] Prins, J. E. J. (2003). Het BurgerServiceNummer en de strijd tegen Identiteitsfraude. *Computerrecht* (1): 2-3.
[585] *Ibid.*
[586] *Kamerstukken I* 2007, 38 1175.
[587] *Ibid.*
[588] *Ibid.* Translation van der Meulen.
[589] *Ibid.* Translation van der Meulen.
[590] Het Expertise Centrum (HEC) (2007). *Papernote 21: Naar een goed gebruik van het burgerservicenummer.*

of the citizen service number, but also states how the government devoted considerable attention to the prevention of such fraud through the design and implementation of the number.[591] Still, HEC identifies the potential risks associated with agencies accepting the citizen service number as a sole means of identification used by citizens.[592] This potential risk is particularly evident in the United States (see section 4.2.1), where the use of a number, and as such the mere knowledge of the number, functions as a means of identity verification.

Whereas originally the government shied away from articulating how the private sector could use the citizen service number, developments led to the need for more concrete decisions. Ever since the introduction of the idea of a citizen service number, the financial services industry has been eager to be involved. In 2005, the Dutch Banking Association proclaimed both its interest in and the necessity for access to the number as an instrument to be used internally by banks for identity verification.[593] The usage of the citizen service number by the financial services sector was projected as a must in the fight against terrorism and money laundering.[594] Boele Staal claimed how access to the citizen service number and the legal duty of care imposed on the financial services sector by the government in the fight against terrorism, money laundering, and fiscal fraud maintained an intricate connection.[595] In an effort to carry out Customer Due Dilligence, banks must also receive the possibility to conduct such activities in a comprehensive manner, according to Jan Berkvens, who also indicates how the Dutch Data Protection Act provides sufficient room for the government to grant banks access to the number.[596] The former Minister of Finances did indicate in 2005 in the Lower House how he planned to grant banks access to the number.

Several years later, in 2009, the government finally introduced a bill to realize the involvement of the financial services sector.[597] In particular the increased emphasis on identity verification in light of anti-money laundering initiatives along with the prevention of terrorist financing provided the government with ample motivation to support the involvement of the financial sector. The government notes how the usage of the number by the financial sector is not a new phenomenon.[598] For tax purposes, banks have a legal obligation to use the citizen service number when providing the tax administration office with information about its clients. The government emphasizes the importance of opening up the usage of citizen service numbers to financial service providers in order for them to obtain a complete picture of their clients and the government anticipates a decrease in errors due to the usage of the number.[599]

In its reaction to the legislative proposal for usage of the citizen service number in the financial services sector, the DPA proved critical.[600] The usage of the citizen

---

[591] *Ibid*: 62.
[592] *Ibid.*
[593] Nederlandse Vereniging van Banken (NVB). (2005). Position paper: Banken en Burgerservicenummer (BSN). Available at: http://www.nvb.nl/scrivo/asset.php?id=18191 (last accessed July 12, 2010).
[594] Dubbeling, E. (2008). Gebruik Burgerservicenummer een 'must' voor banken. *Bank Wereld*, Vol. 2008 (1).
[595] *Ibid.*
[596] *Ibid.*
[597] Wet gebruik burgerservicenummer in de financiële sector (2009). Consultation version. Available at: http://www.minfin.nl/dsresource?objectid=77290&type=org (last accessed July 12, 2010).
[598] Ministerie van Financiën (2009). Memorie van Toelichting. Unofficial version.
[599] *Ibid.*
[600] CBP (2010). Wetgevingsadvies – Wet gebruik BSN in de financiële sector.

service number within any particular sector requires a demonstration of societal necessity. This requirement is set forth in Article 8 of the European Convention on Human Rights. According to the DPA, the government failed to establish and demonstrate a societal necessity in order for the financial services sector to gain the right to access and use the citizen service number.[601] The DPA therefore calls upon the government to provide a more convincing demonstration of the social necessity of the usage of the citizen service number by the industry of financial services.

Before the financial services sector, the healthcare sector managed to successfully obtain access to the usage of the citizen service number.[602] This happened soon after the passage of the citizen service number. The Dutch DPA noted how the Interdepartmental Committee van Thijn stated that when a particular sector deals with 'sensitive' personal information as defined in the Dutch Data Protection Act, such a sector ought not to be allowed to replace its sectoral number by the citizen service number.[603] Medical information is an example of such special personal information. Despite this advice, the Ministry of Administrative Innovation still embarked upon a study to investigate the possibilities for abandoning the requirement of a separate number within the health care sector in an effort to introduce the usage of the citizen service number. Such replacement required certain conditions which aimed to ensure the privacy of individuals. To ensure the privacy aspects of such a proposal, the Ministry called upon the Dutch DPA to provide its assistance. The DPA provided an affirmative advice about the implementation of the citizen service number in the health care sector, but identified several conditions and safeguards to ensure the privacy of individuals.[604] The measures introduced and identified by the DPA in its memorandum should be in place before the actual implementation of the citizen service number in the health care sector. The particular conditions mentioned by the DPA include a proposal which specifically states when and under what conditions actors within the health care sector may use the citizen service number. The DPA also expressed concerns about the manner in which the supervision of the usage of the number was regulated within the proposed bill.[605]

Concrete existing problems with respect to the citizen service number and its predecessor the social-fiscal number are the usage of the number by illegal immigrants for work purposes, as previously noted. As a result, the authentic 'owner' of the citizen service number appears to work multiple jobs and as such earn more money which often invites the tax administration office to commence an investigation or alter the tax bracket. The consumer complaint center has received complaints about perpetrators of identity theft using the citizen service number of the victim which leads to problems with the tax administration office.[606] This type of problem already existed during the era of the social-fiscal number. A study published in 2002 concluded how 49% of its investigations concerned illegal usage of the social-fiscal number.[607] In particular, temp agencies

---

[601] *Ibid.*
[602] Wet gebruik burgerservicenummer in de zorg. *Stb.* 2008, 164.
[603] CBP (2005b). Advies Wet gebruik BSN in de zorg.
[604] *Ibid.*
[605] *Ibid.*
[606] Interview *Centraal Meldpunt Identiteitsfraude*, October 30, 2009, Den Haag.
[607] UWV-GAK (2002). *Project Sofi-nummers 2000 – 2001. Onderzoek naar misbruik en oneigenlijk gebruik van Sofinummers.*

turned out to be involved in many cases of such illegal usage. The incentive for the study proved to be the accumulation of complaints from individuals who receive status updates from the social security agency and discovered employment relations which were not theirs.

4.3 Identification Documents

Personal identity and identification carry an extensive history. Valentin Groebner traces the historical roots of the topic in his book *Who Are You? Identification, Deception, and Surveillance in Early Modern Europe*. Through his historical description, Groebner illustrates how travel documents, especially the introduction of the passport, transformed itself from a privilege to an obligation.[608] Initially, travel documents such as letters of recommendation and safe conduct carried an air of exclusivity because only limited individuals managed to obtain the rather expensive documents for their journeys. Letters of safe conduct and recommendation became more advanced and represent the origins of the current passports used around the globe as a means of identification during foreign travel.

Groebner acknowledges how the validation of the identification document came about through the mark of the sovereign or authority who issued the document. The right to produce such a mark or seal of authenticity rests firmly in the hands of the government. The issuance of identification documents is, according to Groebner, a government monopoly, or at least the government aims to make it so.[609] Groebner's eloquent description is both informative and intriguing due to the resemblance of challenges between the past and the present. The introduction of passports as an obligation rather than a mere privilege made its value enormous. Value of a product, especially when its value rests in its ability to gain access to monetary benefits, undoubtedly leads to crime. Groebner describes how unauthorized access to official seal stamps provided a crucial tool to allow fraudsters to reproduce unauthorized documents. This was, according to Groebner, a common problem in the late Middle Ages. Obviously, this led to authentication problems. The mere reliance on the identification document proved problematic because of the production of unauthorized documents which were indistinguishable from their authorized counterparts. The following solution became common practice, according to Groebner,

"…identification and furnishing proof of a person's authenticity would no longer be rendered possible by the official signs of absent authorities adorning documents that an individual produced. Instead, authenticity in identification was to be achieved by matching such documents with internal registers, replete with information supposedly readily on hand in official archives. In the turn to the modern period, identity documents became more and more closely bound up with area-wide, exhaustive registration systems, at least in official theory. Such is the large historical narrative of expanding control, tightening administration, and 'disciplining' in a period that is said to begin in the fifteenth century and whose fruition is commonly dated in the sixteenth and seventeenth centuries."[610]

---

[608] Groebner, V. (2007). *Who Are You? Identification, Deception, and Surveillance in Early Modern Europe*. New York: Zone Books: 174-175.
[609] *Ibid:* 183.
[610] *Ibid:* 201-202.

This period, according to Groebner, marks the beginning of the modern administration, which countries still cling to in contemporary society.

Other significant international developments increased the importance and the value of travel documents and introduced the 'identification revolution.'[611] Especially the influence of World War I and World War II receive considerable attention throughout historical discussions of passports and their role in society.[612] Whereas increased foreign travel and the need for appropriate documents mainly focuses on Europe, the developments across the ocean also influenced the United States and its decisions.

The identification documents discussed below are more expansive than merely the passport. As a matter of fact, for the United States the focus is exclusively on its driver's license system and in the background on the 'feeder' documents needed to obtain such a license. The section on the Netherlands, in contrast, divides its attention between both the passport and the driver's license due to the significance of both in the national identification infrastructure. Even so, the historical description provided by Groebner maintains its relevancy through the emphasis on the transformation of documents and the challenges posed by the determination of their authenticity and the ability to verify their ownership.

4.3.1 United States

There is no national identification infrastructure in the United States. Instead, the identification infrastructure in the United States depends primarily on state-issued driver's licenses. Driver's licenses in the United States are more than a document which grants an individual the legal right to operate a vehicle. The driver's license functions as a proof of identity for various transactions and services throughout the country. From a logical perspective, such an expansion of functions is quite obvious. The need for a driver's license in the United States is high, certainly higher than in countries where the public transportation system is a realistic alternative. Aside from the urban areas, many parts of the United States do not have a functional public transportation system. The sheer size of the country refutes walking as a viable means of transportation. As a result, the ability to drive is an essential aspect of modern life for many, if not most, Americans. The need for a driver's license for many Americans leads to an expectancy that many actually hold such a document, which makes it a convenient instrument for other purposes, such as identification. Furthermore, the implementation of a separate identification document, such as a national identity card, is both a costly and politically sensitive option. Passports never became the de facto form of identification because Americans only apply for the travel document when they can and want to go abroad. For many Americans, travelling is either not a viable option or an attractive prospective. As a result, passport possession is less common than driver's license ownership. Serge Egelman & Lorrie Faith Cranor express how the driver's license is the most often used form of government-issued identification in the United States.[613] Nevertheless, historically driver's license

---

[611] Noiriel, G. (1996). *The French Melting Pot: Immigration, Citizenship, and National Identity*. Translated by Geoffrey de Laforcade. Minneapolis: University of Minnesota Press.

[612] Torpey, J. (2001). 'The Great War and the Birth of the Modern Passport System,' in J. Caplan & J. Torpey (eds.) *Documenting Individual Identity*. Princeton, NJ: Princeton University Press: 256 – 269.

[613] Egelman, S. & L. F. Cranor (2006). The Real ID Act: Fixing Identity Documents with Duct Tape. *I/S: A Journal of Law and Policy for the Information Society*, Vol. 2 (1): 149 – 183.

administrators did not want the document to be used for anything other than to grant individuals the right to operate a vehicle.[614]

The Tenth Amendment of the U.S. Constitution indirectly grants the individual States the exclusive authority to issue driver's licenses. The Tenth Amendment states that "[t]he powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."[615] Since the right to issue driver's licenses is not expressively delegated to the Federal government in the Constitution, it falls under the authority of the States. Each State has a specific department, agency or bureau which administers the written and practical exams, and subsequently issues driver's licenses.[616] Generally this is the Department of Motor Vehicles (DMV), but is also sometimes called the Motor Vehicle Association (MVA), as in the State of Maryland for example. The organization or the agency or bureau is vastly different from State to State. According to Egelman and Cranor, in most states the DMV is part of the Department of Transportation.[617] In a few exceptions, however, it is part of the Department of Public Safety or the Department of Revenue. Each State has the liberty to determine where the agency is most at home. State legislation dictates the powers and function of the DMV, but individual directors determine what information applicants need to divulge in order to obtain a license.[618] Although sometimes statutes or regulatory agreements determine which information is required from the applicant.

Egelman and Cranor provide a thorough analysis of the requirements to obtain a license in all fifty States.[619] Most States distinguish between primary and secondary forms of identification. Primary forms of identification predominantly include birth certificates and passports. Ironically, the list of secondary identification documents lists items which are normally *not* used for identification purposes such as marriage certificates, social security cards, immigration documents, and even school records. The primary form of identification, especially the use of the birth certificate, is also far from bullet proof. According to Egelman & Carnor, in all States individuals can obtain a license through providing a birth certificate and another document which was obtained through the same birth certificate. The authors, as a result, rightfully acknowledge how "[t]his is a gaping security hole in the identification process as it is trivially easy to obtain a birth certificate."[620] Eight vital records jurisdictions maintain a policy of 'open' records at the State or local level which means individuals without a legal right to a birth certificate may still obtain a certified copy of the birth certificate.[621] Other problems associated with the use of birth certificates include the vast variety in type of certificates issued within the United States and its territories. In total, there are 14,000 variations of birth certificates in 57 United States jurisdictions.[622]

---

[614] Identity Theft Prevention and Identity Management Standards Panel (IDSP). (2009). *Workshop Report Identity Verification*: 9.
[615] U.S. Const., amendment X.
[616] The same agencies, bureaus, or departments also issue a basic, non-driving identity card to those unable to drive.
[617] Egelman & Cranor (2006).
[618] *Ibid.*
[619] *Ibid.*
[620] *Ibid:* 169.
[621] IDSP (2009).
[622] *Ibid.*

This vast variety complicates the ability of individuals to assess the authenticity of the document.

Stephen T. Kent and Lynette I. Millett recognize how "[t]he integrity of any authentication system that relies on a government-issued identifier depends on the integrity of a small number of foundation ID documents issued by government organizations."[623] The authors furthermore note how circular the process is with respect to either obtaining a government-issued form of identification or requesting a duplicate, since the birth certificate can easily be obtained yet is used as a verification document for other applications. Among their most relevant findings is the assertion that "[m]any of the foundational identification documents used to establish individual user identity are very poor from a security perspective, often as a result of having been generated by a diverse set of issuers that may lack an ongoing interest in ensuring the documents' validity and reliability. Birth certificates are especially poor as base identity documents, because they cannot be readily tied to an individual."[624]

The driver's license issue became a greater source of concern after the events of September 11, 2001. The 9/11 Commission determined in its report how "[a]ll but one of the 9/11 hijackers acquired some form of U.S. identification document, some by fraud. Acquisition of these forms of identification would have assisted them in boarding commercial flights, renting cars, and other necessary activities."[625] The 9/11 Commission used this conclusion to introduce the following recommendation "[s]ecure identification should begin in the United States. The Federal government should set standards for the issuance of birth certificates and sources of identification, such as driver's licenses. Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists."[626] The Federal government responded to the recommendation set forth by the Commission and introduced the REAL ID Act in 2005.[627] The Act specifically states how its primary aim is "[t]o establish and rapidly implement regulations for State driver's license and identification document security standards, to prevent terrorists from abusing the asylum laws of the United States, to unify terrorism-related grounds for inadmissibility and removal, and to ensure expeditious construction of the San Diego border fence."[628] Only Title II of the Act, the establishment of regulations for security standards of State driver's licenses and identification documents is pertinent to the issue of financial identity theft. To achieve its aim of security standards, the Act introduces minimum document requirements and issuance standards for Federal recognition. The Act grants States a period of three years after its enactment to adhere to the minimum standards set. This means the Act prohibits Federal agencies to accept driver's licenses or personal identification cards for any official purpose after May 11, 2008 unless the license or card has

---

[623] Kent, S. T. & L .I. Millett (2003). *Who Goes There? Authentication through the Lens of Privacy*. The National Academy of Sciences: 156

[624] *Ibid:* 168.

[625] National Commission on Terrorist Attacks upon the United States (2004). *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*: 390.

[626] *Ibid.*

[627] Pub.L. 109-13, 119 Stat. 231.

[628] *Ibid.*

been issued by a State that is meeting the requirements set forth in the Act. These minimum standards required in order for individuals to use the State issued form of identification for Federal purposes, include the person's full legal name, date of birth, gender, driver's license or identification card number, a digital photograph of the person, address or personal residence, and the person's signature.[629] Furthermore, the Act also requires physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes, and the document must contain a common machine-readable technology, with defined minimum data elements. In addition to the minimum document requirements listed above, the Act also lists minimum issuance standards. The Act draws a distinction between general and special requirements.[630] The State must furthermore adhere to 'Special Requirements' which include evidence of lawful status of the applicant.[631]

In particular these special requirements appear to arouse suspicion about the actual motivation behind the introduction of the REAL ID Act. According to Jim Harper, "[t]he REAL ID Act was nominally aimed at preventing terrorists from entering the country. But this was a rather small fig leaf covering a broader attempt to curtail illegal immigration."[632] Harper continues his argument through the exposition of a historical path taken by the United States Congress to reduce illegal immigration through identification-based surveillance for immigration law enforcement. Due to the availability of false identification papers in the United States, such surveillance proved rather unsuccessful historically. Michael Froomkin echoes a similar conclusion when he writes, "[a]lthough promoted as a way to protect against terrorism, the act's most likely effect will be to make it more difficult for undocumented aliens to forge credentials for employment."[633] The other aspects of the REAL ID Act, which fall outside of the scope of this analysis,

---

[629] *Ibid.*

[630] "In general," the Act states, "...a State shall require, at a minimum, presentation and verification of the following information before issuing a driver's license or identification card to a person:
(A) A photo identity document, except that a non-photo identity document is acceptable if it includes both the person's full legal name and date of birth.
(B) Documentation showing the person's date of birth.
(C) Proof of the person's social security account number or verification that the person is not eligible for a social security account number.
(D) Documentation showing the person's name and address of principal residence.

[631] The Act therefore demands the States to "require, before issuing a driver's license or identification card to a person, valid documentary evidence that the person--
(i) is a citizen of the United States;
(ii) is an alien lawfully admitted for permanent or temporary residence in the United States;
(iii) has conditional permanent resident status in the United States;
(iv) has an approved application for asylum in the United States or has entered into the United States in refugee status;
(v) has a valid, unexpired nonimmigrant visa or nonimmigrant visa status for entry into the United States;
(vi) has a pending application for asylum in the United States;
(vii) has a pending or approved application for temporary protected status in the United States;
(viii) has approved deferred action status; or
(ix) has a pending application for adjustment of status to that of an alien lawfully admitted for permanent residence in the United States or conditional permanent resident status in the United States."

[632] Harper, J. (2006) *Identity Crisis*. Washington, DC: CATO Institute: 145.

[633] Froomkin, A. M. (2009b), 'Identity Cards and Identity Romanticism,' in I. Kerr, V. Steeves & C. Lucock (eds.) *Lessons From the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*. New York: Oxford University Press: 252.

also appear to focus on illegal immigration and the efforts of the Federal government to respond to this problem. The application of the Act to the reduction of financial identity theft appears to be pressed into the background for the primary focus remains on illegal immigration and terrorism. This is strikingly similar to the introduction and subsequent execution of the Identity Theft Penalty Enhancement Act (see section 3.1).

Overall, the REAL ID Act remains a source of controversy. Certain sources labeled the provisions introduced in the Act as a wolf in sheep clothing. Or a national identification card with a different name. Egelman and Cranor argue how "[s]ince all of the new licenses will have the same information on them, which is then stored in one national database, this basically creates a national ID card."[634] Several sources, from privacy advocates to individual States, oppose the mere existence of a national identification card, which complicates the government's implementation of the REAL ID Act. On January 29, 2008, the Department of Homeland Security extended the original compliance date from May 11, 2008 to January 1, 2010. This extension only applied to States who filed for an extension in a timely fashion. This turned out to be all States, according to the Department of Homeland Security.[635] Whereas the Department of Homeland Security emphasizes the benefits provided through the implementation of the REAL ID Act, including an anticipated reduction in cases of and costs associated with identity theft, other sources instead emphasize the costs associated with the REAL ID Act. The Electronic Privacy Information Center (EPIC) has been a pioneer against the implementation of the REAL ID Act. In its opposition, EPIC receives company from other organizations such as the American Civil Liberties Union (ACLU).[636] The objections raised against the national identification card are diverse. These objections are part of a broader criticism about the introduction of a national identification document system (NIDS). Richard Sobel declares how "[t]he creation of a NIDS undermines the basic principles of personhood, sovereignty, due process, and federalism in the U.S. Constitution while ultimately providing questionable utility."[637] Especially the issue of federalism is a crucial aspect of the strong opposition expressed by individual States with regard to the implementation of the REAL ID Act. The Federal government, according to the States, basically surpasses its constitutional powers and undermines the sovereignty of the States. Closely associated with this argument is the lack of sufficient Federal funding which accompanies the requirements, despite the costs anticipated by States in order to carry out the requirements set forth by the REAL ID Act. According to a calculation made by a cooperative effort of the National Governors Association, National Conference of State Legislatures, and the American Association of Motor Vehicle Administrators (AAMVA) the implementation of the REAL ID Act will cost more than $11 billion over a period of five years.[638] The estimation of DHS is lower at $3.9 billion. Even so, Congress only appropriated $200 million for State implementation. This tension between

---

[634] Egelman & Cranor (2006).

[635] Department of Homeland Security (2009). Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes. 6 Code of Federal Regulation Part 37.

[636] See http://www.realnightmare.org/

[637] Sobel, R. (2002). The Demeaning of Identity and Personhood in National Identification Systems. *Harvard Law & Technology Journal*, Vol. 15 (2): 323.

[638] National Governors Association (2006). The Real ID Act: National Impact Analysis. Available at: http://www.nga.org/Files/pdf/0609REALiD.pdf (last accessed July 13, 2010).

Federal and State governments prevails in the discussion, and from a constitutional perspective this appears understandable.

Nevertheless, for identity theft the focus must be on the other arguments set forth by the opponents, as well as the proponents of the Act. In an analysis of the Department of Homeland Security's National ID Program, EPIC states how "[t]he REAL ID national identification system would harm rather than protect privacy and security, and such a system would exacerbate the country's growing identity theft problem. It decreases security to have a centralized system of identification, one ID card for many purposes, as there will be a substantial amount of harm when the card is compromised."[639] This foreshadowing of an exacerbation of the problem appears to be based on the misguided assumption that through the implications of the REAL ID Act the driver's license increases in value. EPIC appears to omit how the driver's license is already 'one ID card for many purposes', as noted above. The REAL ID Act fails to inherently change the system; instead, the Act streamlines the product and issuance requirements. The President of the International Association of Financial Crimes Investigators precisely focuses on this point when he pleaded for a national identification card as a solution for financial identity theft, at least in the physical world. As he noted, "[w]e are already doing it, why wouldn't you want some integrity to the document?"[640] He therefore identifies the integrity of the document, or the lack thereof, as a crucial vulnerability which requires change in order to reduce the problem of financial identity theft.

Other arguments against the establishment of a national identification card focus on historical events. Sobel writes, "[i]dentity systems and documents have a long history of being used for social control and discrimination. Through the Civil War, slaves were required to carry passes in order to travel away from plantations."[641] This is a legitimate fear in particular with respect to the usage of identification documents during World War II (see chapter 3), which Sobel describes extensively. Other examples include the requirement of citizens to carry internal passports during the 1930s and 1940s by the Union of Soviet Socialist Republic, and the requirement in South Africa where the government required black citizens to carry passes which prohibited their free movement throughout the country for over thirty years, starting in 1958.[642] Sobel also refers to the system of identity cards which assisted in the ability to distinguish between Hutus and Tutsis in Rwanda during the civil war. This system played a significant role in the genocide, according to Sobel.[643] Whereas these horrors certainly ought to serve as a pivotal warning, the comparison drawn with regard to the REAL ID Act appears to suffer from a certain level of exaggeration. The REAL ID Act sets forth requirements about standards of an identification document which already exist and is already used as a national identifier. The historical examples depict situations which are of such a different nature that the fear expressed by Sobel appears unrealistic. This is also evident from the seeming lack of concern expressed by civil law countries, especially in Western Europe. As Froomkin notes, "[a]lthough I have not seen it stated in quite these terms, one gets the sense

---

[639] Electronic Privacy Information Center (EPIC) (2008). *REAL ID Implementation Review: Few Benefits, Staggering Costs*: 21.
[640] Telephone Interview March 19, 2009, Washington, DC.
[641] Sobel (2002): 343.
[642] *Ibid.*
[643] *Ibid.*

the western European answer to common-law paranoia about ID card systems would be that if a regime is using ID cards to oppress its people, the problems are much more fundamental than the existence of the cards—and their absence will not pose much of an obstacle to oppression anyway."[644]

Sobel continues his criticism of NIDS through mentioning practical obstacles which complicate the realization of such a system. Sobel states, "[a] federalized NIDS presents large-scale problems because a national ID requires a national ID number..."[645] This is hardly an objection since such a national identification number also already exists de facto, the SSN. Both the driver's license and the SSN function as means of national identification. This is a problem, as financial identity theft painfully demonstrates.

The Real ID Act, despite its controversial nature, is not completely without support. James Jay Carafano is strongly in favor of the Real ID Act. When he refers to both the Intelligence Reform Act of 2004 and the Real ID Act of 2005, Carafano writes, "[t]hese laws are grounded in common sense. Administrators of the American Association of Motor Vehicle Administrators has long recommended similar measures. Requiring more secure documents and procedures for issuance and monitoring is not a 'silver bullet,' but this strategy will help to combat identity theft, fraud, and other crimes."[646]

The future of the REAL ID Act remains rather uncertain. The Department of Homeland Security provided States with an additional opportunity to request an extension for implementation. This moves the compliance deadline up to May 10, 2011 and in the meantime efforts to repeal the Act, both at the State as well as at the Federal level, continue.

4.3.2 The Netherlands

The main alternatives of documentation used in the Netherlands for identification purposes are the passport, national identification card, and the driver's license. The passport system in the Netherlands carries a turbulent history. The period after World War II in particular contains various moments of political and social controversy. Continuous evidence of the document's sensitivity to fraud, advances in technology, international developments, along with the altering landscape of the government in its search of administrative efficiency and effectiveness caused considerable conflict on different occasions. The early passport controversy which occurred during the eighties was mainly a political affair, whereas the more recent disagreement reflects a crucial social dimension. The 1950 passport model became the topic of political concern during the early eighties.[647] The discussion surrounding the introduction of a different passport model maintained two distinct origins. The first were international discussions and developments about the uniformication and standardization of identification and travel documents. This discussion at the international level commenced during the end of the sixties and arose as a result of various developments, including increased travel of citizens around the world and increased cooperation among various countries around the globe.[648] The increased prevalence of fraud through the usage of travel documents

---

[644] Froomkin (2009b): 18-19.
[645] Sobel (2002): 363.
[646] Carafano, J. J. (2008). Making REAL ID Real—Finally. *WebMemo*, Heritage Foundation.
[647] *Kamerstukken II* 1987 – 1988, 20 559, nr. 7.
[648] *Ibid:* 31.

also factored into the discussions and proved to be a crucial reason for the introduction of a European passport. This leads into the second main reason for a reconsideration of the Dutch passport. Internationally, the Dutch passport carried a negative reputation due to its severe sensitivity to fraud which granted those in possession of the document the ability to commit fraud at a global scale. Its negative reputation helped the document obtain the unflattering nickname of 'the black rag.'[649]

Through the ratification of a European resolution on 23 June 1981, the Netherlands officially committed itself to the development of a passport which embodied the uniform model introduced in the European community.[650] The Ministry of Foreign Affairs opened the conversation in 1983 with the State Publisher about a new passport model. A year later, in 1984, the European Union initiated an agreement to design a more fraud resistant passport model at the European level for all Member States.[651] Especially in the Netherlands the need for a more fraud resistant passport appeared eminent. Other issues surrounding the design and ultimate production of the passport complicated the matter. The privatization of the State Publisher appeared to be a concrete possibility, which meant the government gained the liberty to enter an agreement with another corporation. Before the possibility of privatization, the government was required to grant all relevant contracts to the State Publisher. The release from such a requirement led the government to venture elsewhere for the passport production process. Instead of the State Publisher, the government entered an agreement in 1986 with a new corporation KEP, especially established for passport design and production.[652] The government's decision to circumvent the State Publisher and grant the contract to another corporation became an issue of dispute. Many questioned whether the government's decision was particularly wise.

The other more prominent issue which caused considerable concern among members of the Lower House was the quality of fraud resistance the new passport design could offer. The first round of fraud resistance tests came in 1987 and 1988.[653] The Immigration and Naturalization Office (INS) in the United States tested the passport model on its ability to resist attempts at possible falsification. The INS provided an overall positive response to the passport, but made several critical remarks for improvement. When the government sent a letter to the Lower House, it mentioned the positive results but kept the areas for improvement as mentioned by the INS to itself.[654] As political pressure increased, and the introduction of the new passport model continuously found itself postponed, the Lower House requested a study to investigate whether a fraud resistant passport for a reasonable price was actually a viable option.[655] The research results were not negative, since the study results demonstrated how everything should work out as planned. The Lower House, despite the comforting results, required the government to conduct various tests to measure the level of fraud resistance offered by the new passport model. These tests came out negative and fuelled the

---

649 'Parlementaire enquête paspoortproject (1984-1988)' (n.d.). Available at: http://www.parlement.com (last accessed July 14, 2010).
650 *Kamerstukken II* 1987 – 1988, 20 559, nr. 7.
651 *Ibid.*
652 *Ibid.*
653 *Ibid.*
654 *Ibid.*
655 *Ibid.*

political anger on the side of the Lower House.[656] The government failed to negate the fire when it announced another postponement during a debate in 1988. The Lower House initiated a parliamentary research committee to investigate the facts and the responsibilities of the decision making process.[657] Several government officials refused to cooperate with the research project which led the Lower House to change the research committee to a parliamentary survey committee forcing everyone to cooperate and be questioned under oath during public hearings.[658]

The Committee came back with its results on August 29, 1988 and its judgment was fierce. In its comments on the passport inquiry, Henk van Dongen and Abbe Mowshowitz wrote "[t]he story that emerges from the testimony we have examined is very nearly a textbook case of how not to introduce an information system in a complex organization. Witnesses have discussed the passport system as the proverbial blindmen have reported on the elephant. Limited parts of the beast have been described with accuracy and precision, but these fragments do not add up to a coherent characterization of the whole animal."[659]

The ultimate passport failed to receive positive reactions. Its quality improvement in comparison to the 1950 model appeared scarce.[660] During the following years, the passport design remained a sensitive topic and in 1993, five years after its introduction, TNO[661] offered a negative opinion about the document.[662] In particular, TNO determined how the photograph included in the passport was easily removable. Two years later, the Netherlands issued the first passport which incorporated the European model. The government confirmed a 'maximum level of fraud resistance' which included technological aspects to successfully prevent falsification.[663] Despite this maximization of fraud resistance, the following month the Central Investigation Information Service (CRI) declared the ease with which the photograph on the passport could be removed and replaced. The CRI warned for the fraud sensitive nature of the document which led to an emergency debate in the Lower House in October 1995.[664] A couple of months later, more problems surfaced. Individuals were not required to report the loss or the theft of their passport. They could simply apply for another passport which meant people had the ability to generally apply and own multiple passports in the same name. This reflected the procedural vulnerabilities which often remained in the shadow of the product weaknesses. The plagued passport system received even more negative publicity when law enforcement arrested an Iranian citizen with 110 Dutch passports in his possession ready for falsification.[665]

The government introduced yet another passport model in 1997, which aimed to prevent the ease of photograph removal and replacement. The removal of the

---

[656] *Ibid.*
[657] *Ibid.*
[658] *Ibid.*
[659] *Kamerstukken II* 1987 – 1988, 20 559, nr. 8: 2.
[660] *Ibid.*
[661] TNO is an independent research organization.
[662] 'De fraudegevoeligheid van paspoorten' (1999). *Trouw*. Available at: http://www.trouw.nl/krantenarchief/1999/10/06/2413428/De_fraudegevoeligheid_van_paspoorten.html (last accessed July 13, 2010).
[663] *Ibid.*
[664] *Ibid.*
[665] *Ibid.*

photograph caused the letters to crumble on the page; nonetheless, falsification turned out to be possible.[666] After all the bad publicity, the government began its exploration of biometrics as a means to increase the quality of the document. Unlike the previous four passports introduced during the previous decade, the passport introduced in 2001 managed to survive its original term of five years and receive an additional term. Such a success is the result of the transformation the passport experienced as a result of the incorporation of trusted technology.[667] Previously, the government only allowed the incorporation of proofing technology, which meant those in charge of developing the travel document could only introduce means of technology which had already been introduced by others. Such a limitation proved unsatisfactory for those in charge of the new passport and as such they introduced the idea of trusted technology, which meant a higher level of innovativeness. Trusted technology meant that the provider of the technology had to demonstrate and indicate its technological product was highly promising.[668]

The 2001 passport was a model developed in anticipation of future technological advances and potential requirements. The model was ready for potential implementation of the RFID chip and biometric data such as the facial scan and fingerprints.[669] Other signs of authenticity introduced into the model are the second photograph and an emblem. Furthermore, the developing team also introduced a sign of authenticity which incorporated the usage of another sense. On the page which displays the personal information of the passport holder, the material contains a pattern which is sensible when touched by the authorities.[670]

Discussions about the inclusion of biometric data begin in 1997.[671] The continuous battle to design a fraud resistant document along with the fight against look-alike fraud forced the government to fest all of its hope on the more advanced technologies. Particularly the focus on look-alike fraud by the government increases the attention devoted to other means of technology. Look-alike fraud receives considerable government attention in the Netherlands, in particular due to its connection with illegal immigration. To explore the biometric landscape, the government requested an exploratory study to investigate the many aspects of biometrics, including its benefits for travel documents and fraud prevention.[672] After positive results returned, the government began to envision and emphasize the possibilities biometrics could offer in the future for travel documents.[673] Unfamiliarity with the consequences of implementation of such technological elements led the government to embrace a hesitant attitude. Especially the privacy implications and the level of societal acceptance remained unclear. To move forward, the government initiated additional research projects to investigate the appropriateness of biometrics and travel documents.[674] Fingerprints received the most positive results as a tool to combat look-alike fraud, according

---

[666] *Ibid.*
[667] Interview ID Management Centre, October 21, 2009, Den Haag.
[668] *Ibid.*
[669] *Ibid.*
[670] *Ibid.*
[671] *Kamerstukken II* 1998 – 1999, 25 764, nr. 10.
[672] *Kamerstukken II* 1997 – 1998, 25 764, nr. 4.
[673] *Kamerstukken II* 1997 – 1998, 25 764, nr. 7.
[674] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2003). *Onderzoek naar de toepassing van biometrische kenmerken in de Nederlandse reisdocumenten*. Den Haag, Project Biometrie Agentschap BPR.

to the government.[675] And as a result, the inclusion of fingerprints on future travel documents appeared merely a matter of time. At the same time, the Lower House appeared enthusiastic about the potential of biometrics and stressed the need to implement the system in a speedy manner, due to its promising character.

The events of September 11, 2001 influenced the decision making and implementation process. The United States passed the Enhanced Border Security and Visa Entry Reform Act of 2002.[676] And suddenly international developments with regard to biometrics entered a rapid pace and became a prominent topic of discussion in the fight against terrorism. Nearly everyone turned to the leading authority on the matter, the International Civil Aviation Organization (ICAO). The ICAO, which had been conducting research on the inclusion of biometrics in travel documents since 1997, became a dominating force in the international developments. On May 28, 2003, the ICAO concluded its research and endorsed the facial scan as the standard biometric characteristic as part of the ICAO directives for travel documents.[677] Since the Dutch government previously determined the fingerprint to be the most effective type of biometric to combat look-alike fraud, it decided to include both types of biometric information in the design of the new passport. This became standard procedure after the European Union issued a Council Regulation on December 13, 2004 which required all Member States to include facial scan and fingerprints on the chip in travel documents.[678] Ironically, the Dutch government instigated the discussion at the European level before the Regulation appeared. The Netherlands organized a conference in The Hague, 'European Conference for Issuing Authorities of Travel Documents' with the theme 'Exploring the use of biometrics in travel documents.' The conference became the starting point for political decision making about the use of biometrics in travel documents at the European level. As a result of the Council Regulation, the Dutch government no longer needed to pass a national law to legalize the inclusion of biometrics in travel documents. The European Union provided the legal basis for implementation.

To test the practicality of the inclusion of biometrics, the government initiated a pilot in six municipalities in the Netherlands.[679] The government implemented the new passport in 2006. At that time, the passport included a chip which contained the photograph included in the passport along with personal information including name, date of birth, gender, document number, citizen service number, and expiration date. Three years later, the government implemented the fingerprint requirement which became effective as of September 21, 2009. From that moment on, all applicants needed to provide their fingerprints for inclusion in the travel document and in a database. Whereas the first requirement received justification from the European level, the second requirement comes from the Dutch government. The Dutch Data Protection Authority emphasized the privacy implications of the collection and storage of biometric data. The government acknowledged the privacy implications, but found

---

[675] *Kamerstukken II* 2003 – 2004, 25 764, nr. 22.

[676] Pub. L. No. 107-173 (H.R. 3525)

[677] International Civil Aviation Organization (ICAO). (2003). Biometric Identification to Provide Enhanced Security and Speedier Border Clearance for the Travelling Public. *Press Release*.

[678] Council of the European Union (2004). Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

[679] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2005). *2b or not to 2b*: Evaluatierapport biometrieproef 2b or not 2b.

the counterargument of a more reliable and effective application procedure for travel documents an adequate justification for a breach of privacy. Once again, the government emphasized the pressing need to combat look-alike fraud and the societal value of such a fight. Despite the government's continuous justification, the opposition remained.

Next to the inclusion of biometrics, the government initiated other changes in the overall administration of travel documents. The passport production process occurred decentralized through the various municipalities in the Netherlands. Each municipality individually applied the personal data including photograph and signature to the document. This is a critical aspect of the document production process. This decentralized production process and data collection allowed the municipalities to become a genuine service provider for all citizens and was in place since the late eighties.[680] The decentralized process allowed municipalities to develop a service where passports became like a one-hour photo service, basically ready while you wait. Since 2001, the government began to issue passports in a centralized manner and in 2009 the government stated how this centralization process provided a strong increase for the overall security of the production process.[681] The number of false travel documents in circulation decreased as a result of the centralization process, according to the government.[682]

In addition, the government introduced a central online database. In its justification, the government proclaimed how the choice for a central online database of travel document administration is primarily introduced as a result of the need to make the applicant and issuance process more reliable. A second argument in favor of a central database was the diminishing administrative burden on the citizen. Due to the existence of a central database, citizens can now apply for a passport at any municipality. Previously, citizens were obligated to apply for a passport at their municipality of residence. The government furthermore claims there is no breach of privacy as a result of a centralization of the travel document information administration.

The Identification Duty Act lists besides eligible travel documents[683] also driver's licenses as documents which can be used by individuals in the Netherlands for identification purposes. This inclusion is a result of the desire to expand the reach of the law, to reduce administrative burdens, and to increase user convenience.[684] The history of the driver's license is less extensive and turbulent than the passport's history. Until 1924, individuals did not need to pass an exam to confirm their capacity to operate a vehicle and they also did not need to pass a medical examination.[685] To obtain a license, individuals simply needed to establish they were old enough to drive. Legal changes in 1924 introduced the requirement

---

[680] *Kamerstukken I* 2008 – 2009, 31 324 (R1844), C.

[681] *Ibid.*

[682] *Ibid.*

[683] Eligible travel documents include national passport, diplomatic passport, service passport, travel document for refugees, travel document for immigrants, emergency document, and any other document approved by the Minister of Justice of the Netherlands. The Dutch identification card which is accepted by all Member States within the European Union pursuant to the European Agreement on the movement of people between the Member States, which was signed on 13 December 1957 in Paris, is also considered among the classification of eligible travel documents.

[684] RDW (2009). *Het rijbewijs als sleutel tot de overheid. Business case voor een chip op het rijbewijs*. Versie 0.91. Unpublished document.

[685] Lütter, G. & R. van Troost (2006). *De Dataloods and zijn machinekamer; Inleiding tot de GBA*. Alphen aan de Rijn: Kluwer.

for individuals to pass an exam to determine their capacity to operate the vehicle and they also needed to pass a medical exam. Furthermore, the law also established an expiration date for driver's licenses.[686] Years later, in 1986, another important change occurred when mayors received the legal right to issue driver's licenses, along with the Royal Service for Road Traffic (RDW). The most significant change occurred in 1996 when the driver's license officially became accepted as a form of identification. Before 1996, the function of a driver's license was restricted to its main role, which is to serve as a means of proof someone is legally permitted to operate a vehicle. When the driver's license also became an official form of identification, it no longer served an exclusive function. This 'function creep' is similar to the development of the passport described in the previous paragraph. Due to its change in function, the driver's license also began to contain the social-fiscal number of the individual holder.

Another ten years passed before the government changed the model of the driver's license. Since 2006, the driver's license has the size and material of a credit card. The change from the 'pink slip' to a credit card like document improved security of the document and increased its resistance to fraud and falsification.[687] This change in material and size placed the driver's license at an equal level in terms of security with the passport in the Netherlands.[688] The RDW also changed the application process for a driver's license. The process has become nearly 'paperless.' The RDW also transferred from a decentralized to a centralized process, which meant the end of the 'ready while you wait' service.[689]

Other aspects are still under consideration. The inclusion of a chip on the driver's license is such a potential aspect. This consideration is the result of developments at the level of the European Union. The European Parliament and the European Commission introduced a Directive in December 2006 which aims to harmonize driver's licenses among the member states of the European Union.[690] This Directive also provided member states with the option, rather than the mandate, to insert a chip into the driver's license. The intention of such a chip is to strengthen the quality of the document in an effort to improve its resistance to fraud, especially lookalike fraud.[691] The 'free space' on the chip can be used for other purposes as long as the member state obtains the permission of the European Commission. The RDW expressed its desire to examine the possibility for the implementation of a chip as part of the driver's license. This is in particular because of its potential promise to reduce the driver's license sensitivity to fraud. Due to the extensive usage of the driver's license for identification purposes, the RDW considers the 'free space' on the chip to serve as an ideal outlet to function as an electronic identity.[692] This as a result of the special position of the document as a legal means of identification but also due to the exponential growth of usage

---

[686] *Ibid.*
[687] RDW (2007). Jaarverslag 2006. Available at: http://www.rdw.nl/NR/rdonlyres/201237AF-3B3A-49AC-8ABC-E2C4F0C756ED/0/RDW_Jaarverslag_2006.pdf (last accessed July 13, 2010).
[688] *Ibid.*
[689] *Ibid.*
[690] Directive 2006/126/EC of the European Parliament and of the Council of 20 December 2006 on driving licences.
[691] The focus on lookalike fraud is a central feature of the government in the Netherlands. The RDW states how as a result of the verification of the document as opposed to the verification of the person in possession of the document lookalike fraud is a rising means used to commit identity theft (RDW 2009).
[692] RDW (2009).

as a means of identification among the population. According to the RDW, with a distribution of 11 million driver's licenses, the document is the most prevalent type of legal identification.[693] The development of a chip is in line with an overall trend and effort made to strengthen the quality of documents used for identification purposes. This is mainly the result of the pressure exerted by the United States as a result of its fight against terrorism.[694] The RDW refers to the inclusion of a chip on passports within the European Union, as extensively described above. The inclusion of such a chip on the passport also enhances the incentive for the RDW to include a chip on the driver's license, since this is an effort to reduce the potential for displacement of the crime. Since perpetrators shall attempt to displace their efforts to a document which is less difficult to falsify, and without the chip, the driver's license is such a document.

The incorporation of an electronic identity on the free space of the chip also aims to fill a void of electronic authentication in the Netherlands. As shall become clear later on, a high level of authentication for electronic government services is still absent in the Netherlands. The development of an electronic identity on the driver's license therefore manages to accomplish this objective and since the driver's license is the most prevalent type of legal identification used, the RDW deems the driver's license the most likely candidate to serve as an electronic identity.[695]

The changes made to the quality of the product for both the passport and the driver's license are important with respect to the ability to reduce the risk and increase the effort for falsification of identification documents. Even so, these changes must also come accompanied by sufficient safeguards for the procedural aspects of identification documents. Since a lack of such safeguards might lead to a displacement of the problem. As briefly noted above during the historical description of the passport, originally individuals did not need to file a police report to obtain a replacement for their missing or stolen document. Whereas initially individuals managed to approach the municipality for a replacement of their missing document, they must now first visit a law enforcement office in order to obtain a report about the missing document.[696] This report must subsequently be demonstrated at the municipality's office. The municipality must take the report and the law enforcement office must note the missing document as missing in a database to prevent potential fraud with such a document. This change occurred because after the features of the passport changed, the Board of the Attorney General determined how the introduction of the new passport also led to an increase in reports of missing and stolen documents.[697] This increase is worrisome especially since research demonstrates how the number of reports filed by citizens in the Netherlands for missing documents proved particularly high.[698] Between 1996 and 2001, a total of 682,000 documents were reported as either missing or stolen.[699] And in 2001 alone, the total turned out to be 131,000 passports. There is a lack of investigation into repeat reporters. The Military Police

---

[693] *Ibid.*

[694] There is a certain irony about the ability of the United States to exert influence over the quality of identification documents in other countries in contrast to its ability to exert a similar influence within its own borders.

[695] RDW (2009).

[696] *Kamerstukken II* 2005 – 2006, 30 438, nr. 3.

[697] See also *Ibid:* 2-3.

[698] Koninklijke Marechaussee (2003). *Rapport identiteitsfraude en (reis)documenten*.

[699] *Ibid.*

emphasizes the importance of the document for the criminal arena and states how the passport is worth thousands of euros. This is due to the key role played by the passport for illegal immigration, illegal employment, government benefit fraud, and other forms of criminality.[700] On a global level, the Dutch passport carries a reputation as a valuable and reliable document. Moreover, the ease of replacement procedures and the lack of sanctions for the loss of documents proved to be a known vulnerability to the system.[701] The Royal Constabulary notes how the document is especially lucrative for human trafficking purposes.

The RDW recognized a similar worrisome trend with respect to reports about missing and stolen documents. Whereas in 2006, 81,000 documents were reported missing this increased to 91,000 and 97,000 in 2007 and 2008 respectively.[702]

Whereas the legal obligation to file a report when an official identification document goes missing is a means of situational crime prevention, such a requirement places a heavy administrative burden on street police. As a result, the municipality of Amsterdam, along with other partners including the Ministry of Internal Affairs, analyzed potential simplification of the reporting duty.[703] The new envisioned method is for citizens to directly file a missing document report at the municipality office.[704] This is in contrast to the original method where citizens first had to visit the police station to obtain the report before they could request a replacement document at the municipality office. The municipality then continues the cooperation with law enforcement who issues a report which is sent to the home address of the petitioner. This report is required for citizens to pick up their replacement document.[705]

Another aspect introduced as a result of the pilot study is a fraud check. The municipality conducts this fraud check based on fraud indicators to assess whether there is any reason to suspect potential abuse of the system. When there are suspicions, the individual in question receives a letter from the municipality which requests the individual to make an appointment with their local law enforcement office.[706] Law enforcement officials shall interview the individual and investigate the potential abuse. The law enforcement official subsequently reports back to the municipality who in the end decides whether the citizen shall receive a replacement passport.[707] This procedure is exclusively reserved for missing documents. When citizens report a document stolen, a different procedure is followed. Since the theft itself is a violation of criminal law, the citizen must first file a report with law enforcement.

4.4 Electronic Identification

The construction of the information superhighway during the latter part of the previous century also attracted the attention of governments around the globe as they began to develop a presence on the Internet.[708] Jeffrey W. Seifert questions

---

[700] *Ibid:* 23.
[701] *Ibid.*
[702] RDW (2009).
[703] Gemeente Amsterdam & Politie Amsterdam-Amstelland (2009). *Evaluatie pilot Vermissing Document.*
[704] *Ibid.*
[705] *Ibid.*
[706] *Ibid.*
[707] *Ibid.*
[708] Hernon, P. & R. Cullen (2006). 'E-government: Transforming Government,' in P. Hernon, R.

the usual claims about electronic government (e-government) as a recent phenomenon. Seifert describes how certain scholars have traced the antecedents of current e-government initiatives, at least in the United States, back to the 1960s. He refers to Licklinder's writings about the potential for computers to move beyond mere storage units and to evolve into units with interactive capabilities. Despite the significant lapse of time before the actual concretization of these writings, the earlier thoughts managed "...to plant the seed of today's attempt to integrate IT into government processes, which we now commonly refer to as e-government."[709] Peter Hernon and Rowena Cullen describe how initially the presence of governments on the Internet was similar to a minor sideroad, whereas more recently its presence has evolved into a significant part of the superhighway.[710]

The benefits offered to governments through their presence on the Internet are apparent and abundant. Especially the efficiency aspect of the online world attracts the interest of government officials. The e-government phenomenon allows governments to improve the management of government resources and the delivery of services.[711] Many authors acknowledge the benefits governments receive through the implementation of e-government mechanisms. Before the evolution of digital technology, governments needed to conduct manual record keeping which served as a disincentive for the accumulation of excessive amounts of information. Digital record-keeping eliminated such a disincentive. Fred H. Cate even speaks of a new and intense pressure on governments to collect and use personal data. Cate identifies the origin of such pressure as a reflection of "...the conviction that greater reliance on digital data will reduce costs and enhance convenience, speed, efficiency, and accountability."[712] This statement embodies the changes introduced in identification information maintained by the Netherlands as described in section 4.1.2.

Certain authors surpass the mere recognition of benefits associated with the incorporation of electronic aspects and claim how e-government is a necessity for contemporary society.[713] William Fenwick *et al.* argue how the increased and widespread use of information technology in the private sector established the necessity for e-government.[714] Both Cate and Fenwick *et al.* sketch a scene where the pressure on governments to implement e-government infrastructures comes from outside forces, mainly the private sector and developments in contemporary society. Yet, the inherent benefits of e-government for governments certainly also deserve partial credit with regard to the motivation for governments to transform themselves. Many of the developments surveyed above, in particular for the Netherlands, are all part of the move made by the government to introduce a

---

Cullen & H. C. Relyea (eds.) *Comparative Perspectives on E-government*: *Serving today and Building for Tomorrow*. Lanham, MD: Scarecrow Press: 3 – 21.

[709] Seifert, J. W. (2006). 'E-government in the United States,' in P. Hernon, R. Cullen & H.C. Relyea (eds.). *Comparative Perspectives on E-government*: *Serving today and Building for Tomorrow*. Lanham, MD: Scarecrow Press: 25.

[710] Hernon & Cullen (2006).

[711] *Ibid.*

[712] Cate, F. H. (2008). Government Data Mining: The Need for a Legal Framework. *Harvard Civil Rights Civil Liberties Review*, Vol. 43: 435 – 436.

[713] Fenwick, W., John, E. & J. Stimac (2009). The Necessity of Egovernment. *Santa Clara Computer & High Tech Law Journal*, Vol. 25: 427-465.

[714] *Ibid.*

different government which focuses on improved service delivery via the electronic superhighway, or at least the incorporation of technological aids.

But the positives of e-government also come accompanied by various tensions and challenges.[715] The transformation of government requires the development of other means of identification which are compatible to the situation in the online world, where the lack of face-to-face contact is a challenge. As Corien Prins notes, "…as the use of digital communication and interaction spreads, public sector bodies need appropriate mechanisms to meet identification needs. And the specifics of electronic communication require the use of other mechanisms than those applied in the physical world. In order to be certain in an electronic environment that certain rights and obligations are rightfully attributed to citizens, it is necessary to implement certainty and transaction security requirements."[716] The increase in potential opportunities as a result of electronic government services is also accentuated by Costas Lambrinoudakis *et al.* when they write, "[b]y allowing users to access services from virtually anywhere, the universe of ineligible people who may attempt to harm the system is dramatically expanded."[717]

4.4.1 United States

To discover the historical roots of e-government in the United States a return to the first Clinton term is required. Joseph A. Salem Jr. describes how former President Clinton embarked upon his political journey as a president with the promise to reinvent the Federal government.[718] When Clinton entered the White House, in 1993, he established the National Performance Review (NPR).[719] The link between reinvention of the Federal government and the proliferation of information technology became evident early on. Former Vice-President Al Gore remarked, "[i]nformation technology (IT) was and is the great enabler for reinvention. It allows us to rethink, in fundamental ways, how people work and how we serve customers."[720] In 1996, Clinton and Gore introduced a new feature to the White House Website. This feature, Commonly Requested Services, allowed 'customers' to conduct various activities online. Clinton expanded his share in the pioneering of e-government in the United States when in December 1999 he released a memorandum to the heads of executive departments and agencies on the topic of e-government.[721] The memorandum contained several guiding principles along with a list of eleven actions which the recipients needed to carry out. According to Seifert, "[i]n many ways, the December 1999 memorandum

---

[715] Dutton, W. Guerra, G. A., Zizzo, D. J. & M. Peltu (2005). The cyber trust tension in E-government: Balancing identity, privacy, security. *Information Polity*, Vol. 10: 13 – 23.

[716] Prins, J. E. J. (2007). 'National perspectives on e-government and required regulatory change', in J. E. J. Prins (ed.) *Designing E-Government*. Kluwer Law International: 279.

[717] Lambrinoudakis, C., Gritzalis, S., Dridi, F. & G. Pernul (2003). Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy. *Computer Communications*, Vol. 26 (16): 1874.

[718] Salem, J. A. (2003). Public and private sector interests in e-government: a look at the DOE's Pubscience. *Government Information Quarterly*, Vol. 20 (1): 13 – 27.

[719] *Ibid.*

[720] Office of the Vice President. (1997). Access America: Reengineering Through Information Technology; Report of the National Performance Review and the Government Information Technology Service Board. Available at: http://govinfo.library.unt.edu/npr/library/announc/access/intro.html (last accessed July 5, 2010).

[721] Seifert, J. W. (2008). *Reuthorization of the E-Government Act: A Brief Overview*. Congressional Research Service Report for Congress.

represented the Clinton Administration's first concrete attempts to begin implementing e-government government wide. The actions called for in the memorandum reflected the activities and findings learned over the past six years through the National Performance Review, as well as the growth of a critical mass of citizens now using the internet."[722]

Before the release of the memorandum, legislation aimed to move government agencies toward the implementation of e-government already passed. "The enactment of the Government Paperwork Elimination Act (GPEA) in 1998", according to Stephen H. Holden and Lynette I. Millett, "has spurred federal agencies to move quickly toward electronic government."[723] This is a direct result of the GPEA's mandate to "'…preclude agencies or courts from systematically treating electronic documents and signatures less favorably than their paper counterparts', so that citizens can interact with the Federal government electronically."[724] More specifically, the GPEA requires government agencies to provide individuals or entities the option to submit information to or transact with the agency electronically, and to maintain records electronically, whenever possible. Furthermore, the GPEA states that electronic records and their related electronic signatures must receive legal effect, validity, or enforceability.[725] The Act also encourages Federal government use of a range of electronic signature alternatives.

In 2000, the Office of Management and Budget (OMB) provided Executive agencies with the guidance as required under Sections 1703 and 1705 of the GPEA.[726] The guidance aimed to provide answers about, among other things, electronic signatures. This includes the risk factors which agencies must take into consideration during the development of electronic signatures. OMB notes how the usage of electronic signatures depends on the nature of the relationship between the two parties engaged in the transaction. These agency transactions fall into six general categories.[727]

Moreover, OMB notes how all transactions contain varying levels of risk, but emphasizes how "…the highest risk of fraud or repudiation is for a one-time transaction between a person and an agency that has legal or financial implications."[728] Moreover, OMB also provides guidance on questions related to the risk of intrusion based on the type of transaction. These can include one of three types of transactions:

---

[722] *Ibid.*

[723] Holden, S. H. & L. I. Millett (2005). Authentication, Privacy, and the Federal E-Government. *The Information Society*, Vol. 21 (5): 367-377.

[724] Senate Report 105-335.

[725] Government Paperwork Elimination Act (GPEA), Pub. L. No. 105-277, Title XVII

[726] Office of Management and Budget (2000). Implementation of the Government Paperwork Elimination Act. Available at http://www.whitehouse.gov/omb/fedreg_gpea2/ (last accessed July 5, 2010).

[727] These are:
(1) Intra-agency transactions (i.e., those which remain within the same Federal agency).
(2) Inter-agency transactions (i.e., those between Federal agencies).
(3) Transactions between a Federal agency and state or local government agencies.
(4) Transactions between a Federal agency and a private organization such as: contractor, business, university, non-profit organization, or other entity.
(5) Transactions between a Federal agency and a member of the general public.
(6) Transactions between a Federal agency and a foreign government, foreign private organization, or foreign citizen.

[728] *Ibid.*

> (1) Regular or periodic transactions between parties are at a higher risk than intermittent transactions because of their predictability, causing higher likelihood that an outside party would know of the scheduled transaction and be prepared to intrude on it.
> (2) The value of the information to outside parties could also determine their motivation to compromise the information. Information relatively unimportant to an agency may have high value to an outside party.
> (3) Certain agencies, because of their perceived image or mission, may be more likely to be attacked independent of the information or transaction. The act of disruption can be an end in itself.

The GPEA received a follow up several years later when former President George W. Bush signed the E-government Act of 2002 into law.[729] Seifert describes the E-government Act of 2002 as "...the primary legislative vehicle to guide evolving federal IT management practices and to promote initiatives to make government information and services available online."[730] Other sources appear more reluctant to credit the Act with such power. When asked whether the E-government Act of 2002 served as a framework for e-government services, Paul Jaeger hesitated before he politely stated "framework is perhaps a bit of an ambitious word."[731]

The President's Management Council, in cooperation with OMB, endorsed the development of 24 e-government initiatives in October 2001. These e-government initiatives carried the goal to significantly improve the delivery of services to citizens across government agencies. Part of the e-government initiatives was the goal to develop a centralized gateway to verify the identity of the users, through several types of credentials. Through the implementation of various means of multiple authentication, the gateway was meant to support the diverse levels of assurance most likely required for conducting personal and financially sensitive government transactions. The gateway should have facilitated a single-sign-on capability for government services. In order to accomplish this goal, the gateway was to serve as a central point of authentication without actually issuing, maintaining or storing credentials. Those tasks were to be part of a network of electronic credential providers (ECP), on which the gateway would rely. The ECP were to include both government agencies and private sector companies.

In a progress assessment, however, the GAO issued a rather negative report.[732] GAO reported how the General Services Administration (GSA) failed to meet important objectives and milestones during its prepatory phase. GSA was to identify the authentication requirements of Federal agencies and e-government initiatives, but failed to fully meet this challenge. The GAO demonstrates understanding for GSA's failure when it writes, "GSA's modest progress can be understood in light of significant challenges that the agency faces in attempting to build the e-authentication gateway."[733]

---

[729] Pub.L.No. 107-347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803.
[730] Seifert (2008): 4.
[731] Interview, February 6, 2009, Washington DC.
[732] General Accounting Office (2003). *Planned e-Authentication Gateway Faces Formidable Development Challenges.* Report to the Committee on Government Reform and the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House of Representatives.
[733] *Ibid:* 24.

The same issuance year as the report of the GAO, OMB issued a memorandum to all heads of all departments and agencies.[734] In the memorandum, OMB states how "[t]o make sure that online government services are secure and protect privacy, some type of identity verification or authentication is needed."[735] The memorandum therefore is composed as a guidance document for all government agencies and departments. The OMB bases its guidance on standards issued by the National Institute of Standards and Technology (NIST) and on comments received from agency Chief Information Officers.[736] The guidance directs agencies and departments to conduct e-authentication risk assessments in an effort to ensure consistency across the government. To conduct such assessments, OMB identifies four different assurance levels from low for little or no confidence to very high confidence in the asserted identity's validity.

In an effort to determine the appropriate assurance level, OMB describes the necessity to define potential impact categories of authentication errors for particular transactions. The higher the potential impact category the higher the assurance level required in order to maximize the prevention probability with respect to the occurrence of such errors. The guidance emphasizes the need for an assessment both of the potential impact along with the likelihood of the actual occurrence of harm.[737] Such harm categories include:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations.

Overall, the approach as provided by OMB appears to take into consideration important factors in its development of identity authentication for e-government services. Even so, the OMB merely provides guidance and as such the actual implementation remains within the realm of individual agencies.

4.4.2 The Netherlands

The Netherlands became one of the first European countries to introduce e-government programs and initiate study groups with regard to e-government issues.[738] The official start of e-government activities occurred in 1994 when the government launched its first ICT policy initiative through the publication of the 'National Action Program on Electronic Highways: From Metaphor to Action' issued by the Ministry of Economic Affairs.[739] Within the action plan, the government recognized a dual role for itself as umpire and player.[740]

---

[734] Office of Management and Budget (OMB) (2003).
[735] *Ibid.* 1.
[736] *Ibid.*
[737] *Ibid.*
[738] Dutch eGovernment Knowledge Centre (2005). *E-government in the Netherlands: a brief history*. Available at: http://www.todigitalworld.org/dl.php?id=21 (last accessed July 5, 2010).
[739] *Kamerstukken II* 1994 – 1995, 23 900, nr. 20.
[740] Dutch eGovernment Knowledge Centre (2005).

During the following years, the government continued its exploration of e-government developments and also invited the private sector to incorporate its views on the opportunities provided through the introduction of the electronic superhighway.[741] In 1996, the government took its first official step toward the delivery of online services when several ministries introduced the OL2000-project which was "…one of the early drivers in introducing demand-led services for citizens in the Netherlands."[742] The main aim of the OL2000 was the introduction of integrated public service delivery through the idea of a one stop shop through an electronic venue.[743] This online service delivery was not to replace other service delivery channels; instead it was to increase the number of channels through which citizens could communicate with and receive services from the government.

The following year, in 1997, the government reviewed the achievements with respect to the action lines set forth in the first national action program. From the review, the government concluded how there proved to be a need for a subsequent action plan which came about in 1998 through the 'Action Program Electronic Government.'[744] The Action Program focused its contribution on three central themes. These included good electronic accessibility of the government, a better public service delivery, and an improved internal operational management within the national government.[745] Each theme came accompanied by several aims. From a transactional perspective, which is the primary focus herein due to its relevancy to financial identity theft, the second theme deserves a brief moment of reflection. The primary aim of the second theme was to make at least a quarter of the services offered by the government available on the electronic superhighway.[746] In the introduction of the action program, the government recognizes yet again its different roles within the realm of e-government. Whereas the government originally defined its roles in terms of umpires and players, this time the government recognizes a role as umpire and provider, along with a role as player. The dual role of umpire and provider coincides to some extent with the distinction made within this research project between the government as protector and provider.

The developments continued throughout the following years as the government published various documents which outlined the visions on and plans for the implementation of e-government services and applications.[747] In 2000, the government provided a progress reflection through its publication of a memorandum 'The electronic government at the start of the twenty-first century.'[748] At the start of the century, the government had managed to make 18% of its services available online to citizens and 19% to businesses.[749] The government set as a goal for itself to make 25% of its services available via the Internet by 2002.[750]

---

[741] *Ibid.*
[742] *Ibid:* 2.
[743] *Ibid.*
[744] *Kamerstukken II* 1998 – 1999, 26 387, nr. 1.
[745] *Ibid.*
[746] *Ibid.*
[747] See for example De Digitale Delta: Nederland oNLine (1999); *Kamerstukken II* 1999 – 2000, 26 387, nr. 8.
[748] *Kamerstukken II* 2000 – 2001, 26 387, nr. 9.
[749] *Ibid.*
[750] The national government had already surpassed this percentage in 2000, since the national

Among the most relevant publications became the introduction of the idea in 2003 of a different government.[751] In yet another action program, the recently installed cabinet proclaimed its vision on a 'different government.' In particular, the action program declares a need for a modernized version of government which also reconceptualizes the role of the citizen. As a result, the government uses the action program as a means of reflection to encourage the improvement of its public service delivery and set a goal for itself to offer 65% of its services through the electronic superhighway by 2007.[752] This action program also introduced the idea of the one time information provision, where the government, or rather government agencies, are not allowed to ask citizens for personal information when such information is already maintained by the government. This ambition in turn also increased the necessity for identity authentication. The action program therefore declares how in 2004 the government shall introduce a means of authentication for citizens to be used during transactions with the government.

A year after the publication of the vision on a different government, the government also issued a more specified plan in an effort to implement its vision.[753] This was in response to the pressure exerted by the Lower House to make the vision more concrete and result oriented.[754] The accompanying letter of the memorandum demonstrates the emphasis placed by the government on the usage of e-government as an instrument rather than a goal in and of itself.[755] The memorandum offers its insights on seven domains. Several of these domains have returned in previous sections within this chapter. These include the usage of a single number for both citizens and businesses along with a system of basic registrations. The other domains concern the accessibility of e-government, electronic authentication, electronic information exchange, and fast connections between government agencies.[756]

The most relevant domain is electronic authentication. The importance of identity authentication already became pronounced in the memorandum on a different government, especially since the government announced its objective to make more than half of its public services available via the Internet. The follow up memorandum to the different government vision recognizes how the Lower House expressed its desire for a single means of electronic authentication for citizens. In the memorandum, the government specifies various levels of security, including high, middle, and basic. The highest security level can be met through the Public Key Infrastructure standard whereas the middle level of security is met by the systems currently used for Internet banking activities.[757] The basic level merely requires identification number and password as is used for the electronic tax administration through DigiD.

The developments for DigiD officially commenced in 2003. The actual introduction of a means of authentication occurred through a merger of two separate ventures. After six government agencies came together to develop a

---

government already provided 32 % of its services online to citizens and 45 % to businesses. The lack of participation by municipalities therefore leads to a lower overall percentage of electronic service delivery.

[751] *Kamerstukken II* 2003 – 2004, 29 362, nr. 1.

[752] *Ibid.*

[753] *Kamerstukken II* 2003 – 2004, 26 387, nr. 23.

[754] *Ibid.*

[755] *Ibid.*

[756] *Ibid.*

[757] *Ibid.*

manifesto group,[758] they introduced the National Authentication Service.[759] This introduction came as a result of a sense of impatience with the (lack of) developments within the national government. Simultaneously, the Ministry of the Interior worked on a Government Access Service. When both parties joined forces, the official and overarching digital signature became a reality.[760] The government introduced and implemented DigiD, which citizens use since January 1, 2005, to use electronic services offered by the government. DigiD stands for digital identity and is a system shared between cooperating governmental agencies, allowing to digitally authenticate the identity of a person who wants to engage in a transaction with or receive information from the government. The government agencies which subscribe to DigiD continue to grow and the government itself continuous the promotion of the tool in order to encourage citizens to use the electronic channel for the delivery of services. In total, 395 municipalities, along with 5 provinces, and 8 water board districts are connected to DigiD.[761] The authentication tool deserves a close analysis to observe its ability to offer citizens a sense of security and to prevent potential abuse which might lead to incidents of financial identity theft.

To acquire a personal DigiD, citizens need to use their citizen service number. They also need to provide their name, date of birth, address including zip code, and e-mailaddress. The latter is optional and only required if citizens want to receive updates on developments related to DigiD. Citizens receive their DigiD within five days via the post. After citizens receive the code, they must activitate the DigiD via the Internet before they can use it. Whereas at first sight this appears to be a secure system, since the DigiD also requires separate activation after receiving the code via the regular post, hypothetically anyone, from your neighbor to your grandfather, can request a DigiD in your name. In fact, the Dutch Tax Agency, suggested to citizens, who either lost or failed to activate their DigiD, to use the DigiD of their neighbors to authenticate their income tax return forms online, for fear that the forms would otherwise not be submitted before the deadline[762] Afterwards, the government recognized the problematic nature of this statement and changed its policy. The recognition of its mistake came after the advice caused an uproar by others, including members of the Lower House.[763] One member even claimed how this suggestion offered by the Tax Administration was the equivalent of a call for fraud. While certainly this is political rhetoric in action, the suggestion provided to citizens is worrisome especially in light of the value of the digital signature. The Tax Administration attempted to mitigate the uproar through stating how the usage of the DigiD of another person merely served as an instrument to send the tax form. The ultimate responsibility remained

---

[758] These include de Belastingdienst, Informatie Beheer Groep (IB-Groep), Centrum voor Werk en Inkomen (CWI), het Uitvoeringsinstituut Werknemersverzekeringen (UWV), de Sociale Verzekeringsbank (SVB) en het College voor Zorgverzekeringen (CvZ).

[759] Vicus (n.d.). DigiD. Available at: http://www.ketenauthenticatie.nl/digid.html (last accessed July 5, 2010).

[760] *Ibid.*

[761] Voortgangsrapportage e-overheid Najaar 2009 (2010). Available at: http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2009/12/14/bijlage-1-voortgangsrapportage-e-overheid-najaar2009/voortgangsrapportagee-overheidnajaar2009.pdf (last accessed July 13, 2010).

[762] Wijndelts, W. (2007). Overheid erkent fout met DigiD. *NRC Handelsblad.* Available at: http://www.nrc.nl/binnenland/article1785120.ece/Overheid_erkent_fout_met_DigiD (last accessed July 5, 2010).

[763] *Ibid.*

with the original tax filer. Even so, the Tax Administration indirectly suggests how the DigiD itself does not need to remain private or a secret. This is contradictory since DigiD is an access key which can assist potential perpetrators of financial identity theft with the ability to access government benefits in the name of another individual.

The use of DigiD by numerous government agencies is both a blessing and a curse. Its efficiency and convenience is apparent. Citizens use a single authentication tool for a broad range of services and transactions for government agencies. These include the applications for student financial aid, along with applications for healthcare or rent subsidy. Simultaneously, citizens can use the instrument to function as a digital signature for their income tax return. The application of the instrument to multiple agencies within the government increases its value which makes the tool more valuable to perpetrators of financial identity theft.

To use DigiD, citizens use username and password. This constitutes the lowest means of authentication. According to the government, "[i]n most cases, this means of authentication offers governmental agencies sufficient assurance of your identity, in addition to the registered address at your municipality, to which the code is send."[764] For more sensitive transactions, there are two other levels of transaction security. These include the middle and the higher level of security. The government decides which transactions require the incorporation of higher levels of security, whether middle or high.

The medium level of security constitutes the use of username and password and an additional means of authentication. This additional means of authentication is an SMS sent to a mobile phone. This medium level of security came as a result of criticism voiced by the *Gemeenschap Voor Informatie Beveiliging* (GVIB) or the Community for Information Security, which described how the level of security introduced via username and password proved too simple as a means of electronic identification for tax returns.[765] The mere use of username and password provides various potential opportunities for perpetrators of financial identity theft to obtain both. The perpetrator can attack the DigiD user through social engineering, physical robbery, or spoofing DigiD. The perpetrator can also target the DigiD system itself or the browser. Other options include guessing or hacking weak passwords or trying to obtain a Digid in the name of someone else.[766] The usage of SMS authentication became the response to the criticism. Such an instrument of security actually originated at the IB-Groep which covers student financial aid in the Netherlands.[767] The IB-Groep used SMS authentication as part of its electronic service application for student financial aid services.

Public cases about financial identity theft through the use of a DigiD are not readily available. The Netherlands Organisation for Applied Scientific Research (TNO) examined identity criminality in an online setting in 2008 and used four different scenarios to demonstrate how cases of identity theft can occur and which

---

[764] Lodder, A. (2007). eID Interoperability for PEGS. National profile of the Netherlands. iDABC European E-government Services: 14.

[765] Feldmann, E. (2006). DigiD krijgt betere beveiliging na kritiek. Available at: http://webwereld.nl/nieuws/40711/digid-krijgt-betere-beveiliging-na-kritiek.html (last accessed July 13, 2010).

[766] De Koning, P. (2006). Hoe veilig is mijn DigiD-wachtwoord? Presentation available at: https://www.surfgroepen.nl/sites/surf-idm/IdM%20documentation%20open/2006-09-26-GvIB-2-DigidPresentatie1.pdf (last accessed July 13, 2010).

[767] Interview IB Groep, October 5, 2007, Tilburg.

parties are implicated as a result of its occurrence.[768] Scenario 3 involves identity theft in connection to a DigiD. The scenario identifies two brothers, Henk and Hans Konijn. The brothers have not spoken to each other in twenty years. Hans is ill and Henk works twenty hours a week as a store stock assistant. The scenario states how Henk decides to request government benefits in the name of Hans, through the use of DigiD. The scenario furthermore claims how Hans is clueless as to what a DigiD actually is. This statement makes the rest of the scenario confusing and inaccurate, because the authors continue the description through writing how Henk goes through the trash of Hans and finds his DigiD username in the first envelope and the password in the second envelope. Henk subsequently uses this to request government benefits from the unemployment agency. The problem with the scenario description and therefore its applicability is the mistake made. How can Hans have requested a DigiD if he does not know what it is? As the description of the application process above demonstrates, DigiD requires a specific request before it is send to the individual. The only value of the scenario is the demonstration of what perpetrators of identity theft can accomplish through the use of a DigiD, which is, for example, to request unemployment benefits.

The authors also remark how the government as provider could develop a more secure method of delivery of the DigiD. Instead of merely sending it via the post, the government could require citizens to pick up the code at the municipality and to demonstrate identification. This suggestion nevertheless also reduces citizen convenience which reduces its attractiveness as a means of enhanced security. Moreover, the lack of public cases about identity theft through the use of Digid also means the urgency for increased security finds its primary basis in hypothetical threats rather than practical examples.

The highest level of security for the electronic highway envisioned was the e-Nik. The developments of the e-Nik find themselves in the midst of administrative and political discussions, which have led to an impasse for many years. The plan of the RDW, along with other partners, to use the free space on the chip for the development of an electronic identity demonstrates the potential plans for the future.

In the meantime, the government is in anticipation of a renewed version of DigiD which is temporarily referred to as DigidX. This DigidX is to be a renewed and future proof version of DigiD. The improvements of and renewal made to the system primarily concern the modernization of its underlying architecture, but also the maintenance and testability of the authentication instrument.[769]

Other important developments include the passage and enactment of the Act on Electronic Government Communications[770] on July 1, 2004. The government primarily aimed to establish rules to regulate electronic communication between government agencies and citizens, but also among government agencies themselves. The Act provides government agencies with the legal right to use the electronic highway to communicate with citizens as long as they have indicated that they are sufficiently accessible via electronic channels. The same requirement is applicable to communication between government agencies. Furthermore, the Act requires government agencies to ensure an appropriate level of reliability and

---

[768] Welfing, D. J. & P. J. M. Veugen (2008). *Identiteitscriminaliteit in een online omgeving*. TNO Rapport 34463. Draft version.

[769] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (n.d.). DigiD. Available at: http://www.logius.nl/producten/toegang/digid/ontwikkeling/planning/ (last accessed July 13, 2010).

[770] *Stb*. 2004, 214.

confidentiality depending on the content and the nature of the message. Basically, the Act aims to ensure that if electronic communication is a viable alternative for its more conventional counterparts, then such communication must adhere to the same standards and conditions. The Act also refers to electronic signatures, which enhance the level of reliability for electronic communication.

From a service perspective, the government also developed a personal internet page which functions as the main portal for citizens to interact with various government agencies. This project began in February 2006. The main aim of the government was to develop a personal doorway for all citizens in the Netherlands. This main portal, which citizens can access through mijnoverheid.nl (literally mygovernment.nl), offers citizens the ability to view the personal information maintained by agencies subscribed to the site. In addition, citizens can easily find and save services offered by government agencies via the Internet. Through the site, citizens can also commence transactions and trace progress of previous transactions which are in the process of completion. Government agencies, at the same time, can send citizens emails when necessary. And the portal functions via a single sign-on function, which makes it a one stop shop as envisioned by the government during its original plan.[771] To access all of these functions, citizens log on with their DigiD and develop a personal and unique site. Citizens therefore develop a portal which contains only the information pertinent and relevant to them. Through this portal, government agencies can notify citizens of issues such as passport expiration date. For those without the personal internet page, this is generally done via the post.

Overall, the government continuously reiterates the desire to improve its services and also emphasizes the request of citizens for service improvement. This is the main driver behind the production of digital services, along with the government's own interest in the establishment of efficiency. Ernst & Young investigated the satisfaction of citizens with the service delivery of the government, in particular at the municipal level. Citizens proved relatively satisfied with the digital services provided by the government. Overall, they provided the government with a 6.7. This is a lower grade than granted by citizens with respect to services offered in general (non-digital), which is a 6.9. Despite the significant time and energy devoted to the development of digital delivery of services, the participation of citizens with regard to the digital services appears to be lower than expected. This is partially the result of concerns maintained by citizens about the security aspects associated with the digital services. Approximately 20% of citizens questioned indicated their concerns about privacy aspects and the protection offered by the government for their personal information when using digital services.[772] Perhaps there is a sense of validity to this concern.

4.4.3 Analysis

The notion of electronic government inspired both the United States and the Netherlands to speak in glorified terms about improved service delivery. For the

---

[771] All of these services and aspects are listed at: http://www.e-overheidvoorburgers.nl/producten,mijnoverheid-nl (last accessed July 13, 2010).

[772] Ernst & Young (2009). *Burgers en eOverheid: Wat verwacht de burger van de dienstverlening door de gemeente?* Available at: http://www.ey.com/Publication/vwLUAssets/EY_2009_Burgers_en_eOverheid/$FILE/Ernst%20&%20Young_2009_Burgers%20en%20eOverheid_B.pdf (last accessed July 13, 2010).

United States, former President Clinton spoke of 'reinventing government' whereas in the Netherlands the government embarked upon a path which aimed to develop a 'different government.' Both maintained similar intentions with respect to efficiency and improved service delivery. Suddenly, the government, including all of its facets and agencies, felt the need to compete with the private sector in the area of service delivery. Such a reconceptualization of the role of government in contemporary society also led to a redefinition of citizens into consumers. The problem with this focus and the transformation of citizens into consumers remains the aspect of security which at times becomes the neglected stepchild of the debate about opportunities for governments in the field of information communication technology. For security challenges convenience and efficiency, especially since such security aims to increase the efforts and the risks perpetrators must take to penetrate the system. As for the conversion from citizens into consumers, the government appears to forget its own status as a monopoly. For unlike in the private sector, citizens do not have an alternative to the government. Through the conversion, governments potentially find themselves attracted to the same pitfalls as others in the private sector. For as shall become apparent in the following chapter, to maintain customers, and to keep them content, the issues of customer convenience and efficiency receive substantial attention, whereas security at times must bite the dust. This unequal balance between these various priorities is more problematic for governments due to the lack of alternatives for citizens.

Certain sources favor the transformation from citizen to customer. In *Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector*, David Osborne and Ted Gaebler capture the transformation within the governmental apparatus. Especially the aspect of a customer-driven government is encouraged by the authors, since they proclaim how "[d]emocratic governments exist to serve their citizens. Businesses exist to make profits. And yet it is business that searches obsessively for new ways to please the American people. Most American governments are customer-blind, while McDonald's and Frito-Lay are customer-driven. This may be the ultimate indictment of bureaucratic government."[773] The problem with this comparison and the overall argument to make government more, if not exclusively, customer-driven is to lose sight of its role and responsibility as protector. This detachment or separation between the diverse functions of government leads to a conflict of interest, which businesses generally do not face until government interjects as *protector* of the people. The answer is obviously somewhere in between since an entire lack of consideration for the needs of citizens also leads to situation as described by the Dutch National Ombudsman which depicts the situation of the citizen caught in the chains of government.[774] Osborne and Gaebler specifically refer to government actions and behavior which demonstrate active neglect for the needs of citizens. The authors summarize the situation as follows, since businesses need customers in an effort to make a profit, they learn to operate in a competitive environment and listen to their customers. Whereas this is true, businesses in the end act out of self-interest, whereas *ideally* the State is to act in the interest of its citizens.

---

[773] Osborne, D. & T. Gaebler (1992). *Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector*. Reading, MA: Addison-Wesley Publishing Company, Inc.

[774] De Nationale Ombudsman (2009). *De burger in de ketens*. Verslag van de Nationale ombudsman over 2008.

4.5 Conclusion

The government as provider is a pivotal actor in the overall establishment of the identification infrastructure in both the public and the private sector. This makes its role fundamental with respect to the opportunity structure of financial identity theft. The identification information maintained by the government is an attractive target for the first stage of financial identity theft and as such the means of information security invoked by the government are of the essence. The spree of data security breaches in the United States plagued both the private as well as the public sector. This demonstrates the vulnerability of the identification information maintained by various agencies within the public sector in the United States. The previous chapter reviewed the evolution of data security breach notification legislation which is relevant to these incidents, and as a result demonstrates the inherent connection between the government as protector and as provider. Michael Froomkin reflects on the exceptional nature of personal information maintained by the government when he writes "[p]rivate data held by the government is not the same as private data held by others. Much of the government's data is obtained through legally required disclosures or participation in licensing or benefit schemes where the government is, as a practical matter, the only game in town. These coercive or unbargained-for disclosures impute a heightened moral duty on the part of the government to exercise careful stewardship over private data. But the moral duty to safeguard the data and to deal fully and honestly with the consequences of failing to safeguard them is, at best, only partly reflected in state and federal laws and regulations."[775]

The element of identification information maintained by the government increases in importance as its accessibility expands. The developments in the Netherlands with respect to the identification information maintained by the Municipal Personal Records Database therefore also come accompanied by various risks, since the information becomes available through the Internet. Such accessibility is a response to the need for more efficiency and convenience, but enlarges potential opportunities for perpetrators. The electronic accessibility of the GBA-V provides a central point of vulnerability since the previously decentralized storage of identification information maintained by the Municipal Personal Records Database becomes centralized.

Besides the potential issuance of identification information, the government also establishes the identification infrastructure which both the public and the private sector depend on through the issuance of identification numbers and documents. Especially in the United States, the facilitation of financial identity theft through the usage of its identification number infrastructure is apparent. The function creep which dominates the usage of the SSN is among the most widely recognized facilitating factors in the United States. The availability of the number paired with its value as an instrument of authentication have played a vital role in the facilitation of financial identity theft. This is after all, from a criminological point of view, due to the accessibility of the target and its value in transactions. This facilitation also demonstrates how the role of government as provider has a spill-over effect into the realm of the financial services industry. The groundbreaking research conducted by Acquisti & Gross also demonstrates the

---

[775] Froomkin, A. M. (2009). Government Data Breaches. *Berkeley Technology Law Journal*, Vol. 24: 1019 – 1020.

ineffective nature of attempts to limit the disclosure of the number, since perpetrators can predict SSNs based on publicly available data. Moreover, the main problem is not the availability but rather the usage of the number as part of the identification infrastructure. This is precisely why in the Netherlands the risks presently appear to be limited; for the number is available but it does not appear to be used as an instrument of authentication in either the public or the private sector. Even so, the historical developments in the Netherlands foreshadow potential problems. For the original and persistent resistance against the evolution of the social-fiscal number into a general number became irrelevant due to the actuality in practice. When the government came to terms with these developments during the early years of the twenty-first century, the government accepted such a state of affairs and officialized it through the introduction of a citizen service number.

The third aspect of the identification infrastructure discussed in this chapter is the collection of identification documents. Much attention has been devoted to the quality of identification documents along with the quality of the issuance process. This especially since identification documents form such an important pillar of the identification infrastructure. This is the aspect where perhaps the cultural differences between the United States and the Netherlands are most pronounced. The driver's license system in the United States is vulnerable to manipulation. This is in part the result of the reliance on birth certificates as a primary source of identity verification whilst such birth certificates are obtainable by perpetrators of financial identity theft. The awareness of a problem is widely carried but widespread agreement about its solution is absent. The REAL ID Act remains a legislative instrument caught in the middle of severe controversy.

The situation in the Netherlands is vastly different; for its political system is accustomed to national means of identification. Moreover, the influence of the European Union also requires the Netherlands to meet certain standards for the quality of the document. Despite its turbulent history, the system of identification documents seems to have recuperated well. Attention is devoted to various aspects of the process including the issuance and the response to missing documents. This is an integral aspect since the financial services sector depends on the integrity of the issuance process as well as the quality of the document during its service delivery and identity authentication of clients.

The developments with regard to the driver's license in the Netherlands also connect its importance to another aspect of the identification infrastructure described in this chapter which is electronic authentication. Whereas the description of a layered security architecture by both the United States and the Netherlands demonstrates an awareness about the necessity for different authentication means depending on the nature of the transaction, the pressure to make electronic means of authentication also convenient is important to bear in mind, since such a pressure may well compete with the security interest. This especially as the result of the transformation from citizens into customers which depicts the transforming role governments began to play as e-government capabilities evolved throughout the years.

5 | Financial Service Providers

The driving force behind financial identity theft is the acquisition of financial assets. Money is the main motivator. Perpetrators of financial identity theft predominantly acquire these financial assets from financial service providers.[776] This demonstrates the vital value of financial service providers in the overall problem of financial identity theft. The significance of financial service providers is evident; yet, the role and associated responsibility of financial service providers is often a source of conflict and inconsistency. This conflict centers around the question whether financial service providers embody the role of victim, villain, or both with respect to identity theft. Throughout the literature, especially in the past, financial service providers have received empathy due to financial losses suffered as a result of identity theft. To many, financial service providers are the *true* victims of financial identity theft. Through the rise of critical academics[777] and interest groups[778], the potential facilitation, or the villain aspect, of financial service providers stepped out of the 'victim's' shadow. Since the acknowledgement of the facilitation of financial identity theft by financial service providers gained more prominence, the business practices used to realize such facilitation also became the object of increased scrutiny. Financial service providers predominately include banks and credit card companies. Other relevant actors included in this chapter are supervisory organs and consumer reporting agencies since their involvement in the financial world, and therefore their inclusion in this chapter, assists in the development of a more comprehensive image of the relevant interactions in the financial services sector. Furthermore, their inclusion is also vital for the background descriptions of various developments with regard to business practices. This chapter reviews business practices based on three different phases including the acquisition of clients, the application process, and account activity of existing clients. The first two aspects are particularly relevant for the potential facilitation of true name fraud, whereas the last phase predominantly concerns account takeover.

5.1 Acquisition Process

5.1.1 The United States

The historical background of the credit card, especially its origins and subsequent evolution, provide important background information for the unfolding story of financial identity theft. The history of the credit card portrays its original luxurious nature through the story of the Diner's Club Card. This card established the *formal*

---

[776] Perpetrators of financial identity theft can also acquire government benefits as noted in the previous chapter.

[777] See for example LoPucki, L. M. (2001). Human Identification Theory and the Identity Theft Problem. *Texas Law Review*, Vol. 80: 89 – 134; Solove, D. J. (2003). Identity Theft and the Architecture of Vulnerability. *Hastings Law Journal*, Vol. 54: 1227 – 1273; Hoofnagle, C. J. (2005). 'Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors,' in A. Chander, L. Gelman, M. J. Radin (eds.) *Securing Privacy in the Internet Age*. Stanford, CA: Stanford University Press; Hoofnagle, C. J. (2009). Internalizing Identity Theft. *UCLA Journal of Law & Technology*, Vol. 13 (2): 1 – 36.

[778] Privacy Rights Clearinghouse, Identity Theft Resource Center, and the Electronic Privacy Information Center.

beginning of the credit card industry in New York City in 1950. James B. Rule describes how "[i]ts inventor's original inspiration was to alleviate the need to carry large amounts of cash to cover meals in that city by providing a single credit card for 'charging' bills in a number of restaurants."[779] The Diner's Club Card gained immense popularity and began to spread its wings, both to other cities and to other types of transactions. The astonishing success of the Diner's Club Card received recognition and paved the way for two 'imitators', the American Express Card and Carte Blanche, in 1958.[780] The curious aspect of the origins of the credit card and its industry is its exclusive appeal and availability to upper-middle class clientele. This changed through the growth of the industry and the introduction of bank credit card schemes. Corporations desired to extend credit privileges on a mass basis to make their practices more profitable and to succeed in a competitive environment. As John C. Weistart notes, "[s]ince each issuer of a multipurpose card potentially could reach a greater share of the credit card market, competition throughout the industry intensified."[781] Such a transformation of the credit card and the competitive nature of the industry inherently influenced the acquisition of clients. For mass acquisition required credit issuers to turn to marketing schemes in an effort to attract clients.

This marketing occurred through the use of mass mailing lists, where the industry distributed unsolicited credit cards to consumers all over the country. The 'unsolicited' aspect of the credit card implies the recipients did not file an application nor did they in any other way request the credit card. The unsolicited nature of the credit cards introduced problems for the industry. Robert M. Smith reported in the *New York Times* on the National Postal Forum III held in 1969, where many industry and postal officials gathered to exchange insights about the challenges of these marketing practices.[782] Several bankers expressed their dissatisfaction with the mass distribution of unsolicited credit cards. This primarily due to the theft of the credit cards from mailboxes. Thomas R. Kennedy recognizes the essential problem of the marketing instrument when he writes, "[t]he lead time given to thieves through the theft of unsolicited credit cards makes them valuable to them, not only in providing funds, but in providing identification."[783] This is a crucial observation in light of financial identity theft. Despite the absence of statistics at the session, the bank security directors in attendance at the Forum emphasized the severity of the problem. When an audience member inquired about the business practice and declared how she threw away all unsolicited credit cards she received, William Thornhill from the First National Bank of Chicago responded "[c]ompetitive situations mean that sometimes you have to temper what you think is the right thing to do."[784] The competition for the acquisition of clients dominated business practices and as a result companies felt compelled to introduce marketing instruments with apparent security challenges. The distribution of unsolicited credit cards paved the way for comical anecdotes which painfully exposed the problematic nature of the

[779] Rule, J. B. (1974). *Private Lives and Public Surveillance: Social Control in the Computer Age*. New York: Schocken Books: 226.
[780] *Ibid.*
[781] Weistart, J. C. (1972). Consumer Protection in the Credit Card Industry: Federal Legislative Controls. *Michigan Law Review*, Vol. 70: 1476.
[782] Smith, R. M. (1969). Unsolicited Credit Cards Bother Bankers, Too. *New York Times*, September 9, 1969: 18.
[783] Kennedy, T. R. (1969). The Plastic Jungle. *Montana Law Review*, Vol. 31: 38.
[784] Smith (1969): 18.

marketing instrument. Kennedy describes the story of Tony Benitez, from Tampa Florida, who was never able to use either one of his unsolicited credit cards. This was a result of the fact that "Tony is five years old and he can't sign his own name, although his credit rating is excellent according to the bank that mailed the credit cards to him."[785] Similar stories describe the tale of nine year old Roger Gelpey of Marblehead, Massachusetts, who managed to buy a one dollar tie with his unsolicited credit card. He completed the tie purchase after he had been turned down for a three hundred dollar loan. And then the more relevant complications surface, as Kennedy continues his anecdotes. He describes the story of a 96-year old widow in Lima, New York who never used her unsolicited credit card, but still received a bill for $1,661.[786] Someone else managed to capture the card for a spending spree.

Businesses began to experience resistance when the problems associated with the distribution of unsolicited credit cards captured the attention of the United States Congress.[787] Senator McIntyre declared how "[t]he mailing of unsolicited credit cards invites theft and fraud, and exposes consumers to unnecessary threats against their solvency and credit standing."[788] Previously the regulation of the credit card industry was minimal, but the unpopular marketing scheme of the industry increased a desire and an urgency for regulation. When Congress began to introduce legislation, it stumbled upon opposition from the Federal Reserve Board and the credit card industry. Both of these parties objected to all proposals made by Members of Congress. The basis of their objection was that there was no major problem with the distribution of unsolicited credit cards that could not be corrected through a more careful screening of mailing lists.[789] Congress disagreed. In August 1967, Representative Wright Patman introduced the first proposal in the House of Representatives for regulation of the industry.[790] The proposal focused primarily on the distribution of unsolicited credit cards. The initial proposal only captured the marketing practices of banks, but later on other credit card issuers also became the subject of regulation. The main initial focus on banks appears to be the result of the correlation between the birth and growth of credit cards as part of the banking industry and the association with the distribution of unsolicited credit cards.[791] The proposal for regulation evolved into an amendment to the Truth in Lending Act.[792] The amendment prohibited the distribution of unsolicited credit cards and specifically states "[n]o credit card shall be issued except in response to a request or application there for."[793] Exceptions to the prohibition include the issuance of a credit card renewal or the replacement of a credit card.[794]

---

[785] Kennedy (1969): 29.
[786] *Ibid.*
[787] Weistart (1972).
[788] Qtd. in email correspondence from Michael D. Gerhardt to Jennifer J. Johnson (2005). Available at: http://www.federalreserve.gov/SECRS/2005/August/20050830/R-1217/R-1217_215_1.pdf (last accessed July 13, 2010).
[789] Kennedy (1969).
[790] Weistart (1972).
[791] Rogers, J. S. (2003). Forged Facsimile Signatures and Basic Principles of the Law of the Check Collection System. Bepress Legal Series, paper 24.
[792] Weistart (1972).
[793] 15 U.S.C. 1642 (1970).
[794] *Ibid.*

Furthermore, the amendment also excludes an associated marketing instrument employed by the industry, the 'negative pre-mailer.' The negative pre-mailer consisted of a printed promotion which announced to the recipient that a card would be sent unless the recipient took *affirmative* action to decline the offer and inform the credit card issuer. The negative pre-mailer introduced a legal predicament in light of the government's aim to regulate the credit card industry. According to Weistart, Congress clearly precluded negative pre-mailers as part of the prohibition. The government therefore indirectly expressed its permission with respect to all solicitations which require the recipient's participation in a plan. Weistart notes, "[a]s long as affirmative action by the recipient is required to trigger the issuance of a card, the contact will not violate the statutory prohibition."[795] The single bill introduced in the House of Representatives to prohibit negative pre-mailers in addition to the distribution of unsolicited credit cards received little attention and failed to gain any prominence. The survival of negative pre-mailers also influenced the evolution of negative option marketing. Peter Bowal describes a state of affairs where the government displays a considerable reluctance to regulate negative option marketing.[796] Despite the overall idea of a sovereign and autonomous consumer in a market-driven economy, consumers fail to attain protection in the area of negative option marketing. Bowel defines negative option marketing as the engagement of a marketer who tenders to the public a product or service and declares the passive acquiescence of the consumer in face of that tender as a form of contractual acceptance.[797] The use of negative pre-mailers creatively circumvents the prohibition set forth by Congress and grants the industry the liberty to continue employing marketing tools which potentially endanger consumers. Even with negative pre-mailers, there is still an additional exposure to financial identity theft because the unsolicited arrival of a credit card forms an opportunity for a perpetrator to take advantage. The industry may defend itself through the printed promotion which grants recipients the option to opt-out and decline the offer, but this places a burden on consumers.

Besides the survival of negative pre-mailers, the industry also developed alternatives to unsolicited credit cards. Such an alternative is the distribution of pre-approved credit card applications which anyone over the age of 18 in the United States may receive. Credit card companies and banks send out massive amounts of these pre-approved applications. These applications already contain the name and address of the recipient and merely require the recipient to sign the form. The recipient then sends the form back to the bank or credit card company to instantly receive the card. The confirmation of the application and the subsequent issuance of the credit card occur instantly due to the pre-approved status of the application. Many of these pre-approved credit card applications provide a limit which is commensurate to the recipient's credit rating and can be relatively low (i.e. 500 or a 1000 dollars), but they can prove to be a stepping stone for larger financial damage. Furthermore, for consumers with a particularly attractive credit history, the credit limits of pre-approved credit card applications may be considerably higher since the risk of late or defiant payments is lower. The excessive number of applications often means consumers discard them without,

---

[795] Weistart (1972): 1504.
[796] Bowal, P. (1999). Reluctance to regulate: the case of negative option marketing. *American Business Law Journal*, Vol. 36 (2): 377 – 390.
[797] *Ibid*: 378.

for example, shredding them. These pre-approved applications are an attractive tool for perpetrators of identity theft. Just as in the past, perpetrators use these marketing instruments to easily obtain a credit card without the knowledge of the rightful recipient.

Unlike the unsolicited credit cards and the negative pre-mailers though, the problem with pre-approved credit card applications is magnified due to another business practice. As Frank W. Abagnale notes, "[i]n today's hotly competitive financial marketplace, speed is of the essence. Thieves love fast credit approval, because haste is the enemy of accuracy. Credit card issuers, for their part, can be very sloppy in doling out cards, failing to match Social Security numbers and dates of birth and otherwise failing to take basic precautions in their eagerness to get cards in circulation."[798] Abagnale, among others, recognizes how many credit card companies claim their screening process is 'tight' and bullet proof, but that certain (media) stories have proven quite the opposite. One of the more famous stories to prove the rather inaccurate verification mechanisms of credit card companies is the story of Clifford, a dog who managed to apply for a credit card. Clifford's owner, Steve Borba, opened up an email account using his dog's name. As time passed, he received a pre-approved credit card application in his email inbox. For Clifford's social security number, Borba used 9 zeros and he explicitly wrote on the application that Clifford was indeed a dog. Despite this comment and the seemingly impossible Social Security Number, Clifford received his credit card three weeks later.[799]

The marketing instrument of pre-approved credit card applications is therefore exacerbated due to the inadequate verification of the application. This occurs due to the automated reading of the application. The automated system is efficient and convenient for the industry and to some extent for its customers, but fails to alert the provider to potential errors. The anecdote above, which is merely an example, therefore also concerns another business practice, namely the application process within the financial services industry. This aspect will be discussed in the following section.

5.2.2 The Netherlands

As described above, the United States introduced the credit card into contemporary society. Despite its international appeal, the Netherlands never became a 'credit card country.'[800] The unpopularity of credit cards in the Netherlands occurred mainly as a result of the well functioning payment by giro system. This offered citizens in the Netherlands an alternative to cash which appealed to them. Simultaneously, the banking industry refrained from any involvement in the credit card industry until the end of the 1970s. For the more affluent citizens in the Netherlands, Diner's club and American Express were available. The banks in the Netherlands began to demonstrate interest in the industry in 1980 and bought the shares of Eurocard Nederland B.V. During the early 1980s, there were less than 200,000 credit cards in the Netherlands.[801] The actual breakthrough for the credit card came in 1988, when the VSB bank bought

---

[798] Abagnale, F. W. (2007). *Stealing your life: The ultimate identity theft prevention plan*. New York: Broadway.
[799] Hoofnagle (2005).
[800] Kosse, A. (2009). *Creditcargebruik in Nederland: Een onderzoek naar de beleving en het gedrag van Nederlandse Consumenten*. De Nederlandsche Bank.
[801] *Ibid.*

the rights from the Bank of America to issue VISA cards to a large audience. Other banks responded and began to issue relatively cheap Eurocard credit cards to the general public.

According to available data in 2007, there were 6 million credit cards in the Netherlands. Actual credit card usage in the Netherlands remains relatively low, approximately 1 % of all transactions in the physical world occur through the use of a credit card.[802] The survey conducted by the Dutch Central Bank concluded how 55 % of the consumers surveyed possessed a credit card. Such a possession was mainly the result of the need to conduct purchases via the telephone, the Internet, and abroad. Many respondents did not express an inherent desire to own a credit card. This is mainly due to availability of alternative methods of payment and the lack of desire to spend money which they do not have at the time of purchase.[803] The usage of credit cards via the Internet mainly appears to occur due to the restricted alternatives offered by various websites. The increased efficiency and speed also plays a role for consumers in the Netherlands, but only marginally. In general, Anne Kosse concludes, based on the survey and its results, how postponed payments and making purchases based on credit is not in the 'nature' of the Dutch. Not even loyalty programs, where consumers can collect miles through the usage of a credit card, appear to overcome this obstacle. As a result, mass acquisition of clients for credit cards never seemed to appear on the horizon in the Netherlands and Kosse does not anticipate it for the future. Through the alternatives offered within the Netherlands, the credit card fails to demonstrate a mass appeal. Furthermore, since the introduction of the Single European Payment Era (SEPA) is expected to lead to the acceptance of the Dutch *pinpas*, or debit card, across SEPA the interest in credit cards shall not significantly increase in the near future.[804]

5.2 Application Process

5.2.1 The United States

The application process to acquire a credit card, open a bank account, or apply for a loan is a crucial stage for perpetrators of true name fraud. The credit card provides direct access to goods and services in the name of the victim, a loan in turn provides direct cash, whereas the bank account is a foundation for future operations. For the credit card industry, the problems associated with the application process became evident in a limited manner through the description provided above about the pre-approved applications. The verification mechanisms used for those applications proved appalling through anecdotal evidence. The problems present in the verification of applications from prospective clients contain historical roots which date back to the first bank credit card scheme to become successful on a large scale. This was the BankAmericard, which originated in 1959. Unlike the other credit card issuers, BankAmericard proved determined to extend credit privileges on a mass basis. Through this determination, BankAmericard has always made it as easy as possible for prospective clients to obtain cards.[805] Especially the application process needed to be easy in an effort to

[802] *Ibid.*
[803] *Ibid.*
[804] *Ibid.*
[805] Rule (1974): 229.

accumulate as many clients as possible. The focus therefore was on the mass acquisition of clients, regardless of their background. The low threshold for approval made the application process and the acquisition of a BankAmericard lucrative, both for legitimate as well as illegitimate clients. The emphasis placed on the simplicity of the application process as a means to obtain as many clients as possible is the result of an 'endemic dilemma.' Rule describes how "[a]ny viable credit-granting policy must deal with an endemic dilemma: stringent standards in the screening of applications can cut losses from bad debts to virtually nil, but result in very low sales volume; indiscriminate acceptance of credit applications, on the other hand, will generate high volume but also unacceptably great credit losses."[806] BankAmericard, according to Rule, "...ran very seriously foul of this dilemma when it began its operations in 1959."[807] BankAmericard began to allocate a significant number of cards without proper discrimination. The card issuer drew wholesale from lists of Bank of America account-holders, consumer reporting agency files, and many other sources. According to Rule, the results of the BankAmericard practices became disasterous. The 'irresponsible' use of the cards by the many cardholders led to considerable losses for BankAmericard and nearly led to its demise. Other similar efforts which ran bank credit card schemes suffered the fate BankAmericard managed to escape.[808]

Even so, Peter Burns and Anne Stanley identify the application process for credit cards as the first line of risk management defense. According to Burns and Stanley, credit card issuers generally confirm an applicant's information through multiple data sources. The specific origin of the data sources used remains unclear. Burns and Stanley furthermore state how "[m]any issuers may also do phone address/distance calculations to determine if the phone number on the application matches the address as defined by the area code on the application. Certain high-risk applications may be pulled for a detailed review depending upon the channel used, the applicant's geographic location or other special characteristics."[809] The credit card issuers also check the information provided on applications with the information provided by the consumer reporting agencies to check for inconsistencies. This cross-reference mechanism is subject to considerable vulnerability due to the inaccuracies present in the information maintained by consumer reporting agencies (see section 5.3).

Burns and Stanley also indicate the presence of additional means of verification during the activation process of the credit card. This occurs through the assessment of the telephone number used to activate the card. When such activation occurs from a telephone number other than the home number listed on the application, the credit card issuer may become suspicious. The credit card issuer can transfer the client to a customer service representative under such circumstances instead of automatically activating the credit card.[810] The customer service representative then tries to verify the identity of the caller through the information listed on the application or the information obtained via consumer reporting agencies.

---

[806] *Ibid*: 197.
[807] *Ibid*: 232.
[808] *Ibid.*
[809] Burns, P. & A. Stanley (2002). *Fraud Management in the Credit Card Industry*. Discussion Paper Payment Cards Center, Federal Reserve Bank of Philadelphia.
[810] *Ibid.*

Despite the elaboration of Burns and Stanley on the efforts initiated by the industry, others emphasize the inadequacy of the means of verification employed by credit card issuers. As Chris Jay Hoofnagle argues, "...credit grantors do not have adequate standards for verifying the true identity of credit applicants. Credit issuers sometimes open tradelines to individuals who leave obvious errors on the application, such as incorrect dates of birth or fudged Social Security Numbers."[811] At the same time, Lynn M. LoPucki states how "[t]he problem is not that thieves have access to personal information, but that creditors and credit-reporting agencies often lack both the means and the incentives to correctly identify the persons who seek credit from them or on whom they report."[812] Both Hoofnagle and LoPucki identify the vulnerability present in the application process conducted by credit issuers. Moreover, Hoofnagle emphasizes how the credit card industry maintains compelling incentives to quickly open a new account which is why part of the industry automates the process.[813] These compelling incentives often lead to a swift process which fails to incorporate 'basic' identity theft prevention strategies.[814]

The endemic dilemma as identified by Rule hence still dominates the business model of the credit card industry, for the companies continue to operate in a fiercely competitive environment which makes the acquisition and acceptance of clients more imperative than the certainty of the applicant's identity. Jeff Sovern confirms this assertion when he describes how the credit industry seems willing to assume the losses suffered through bad debts caused by perpetrators of identity theft because of the benefits that flow from easily available credit.[815] As Hoofnagle eloquently summarizes, "[t]he 'miracle of instant credit,' the ability of anyone almost anywhere to apply for and obtain a new account in seconds, has a dark underbelly – the miracle of instant identity theft."[816] Hoofnagle provides an empirical basis for his observation through an analysis of credit (card) applications completed by perpetrators in the name of the victim. Hoofnagle analyzed 16 fraudulent applications from six victims. In an overview of the most common errors provided on successful applications completed by the imposters, Hoofnagle identifies 12 instances of the wrong address, 3 instances of the wrong phone number, 4 instances of the wrong date of birth, and one instance of the wrong Social Security Number.[817] These are errors which the credit issuer failed to notice during the application verification process. Other observations made by Hoofnagle include significant physical differences between imposters and victims. This is relevant since in-person interactions occurred between the imposter and the credit issuer, who apparently disregarded the noticeable physical differences.[818]

For the banking industry, the Federal government became involved in the application process through the introduction of the Currency and Foreign Transactions Reporting Act, better known as the Bank Secrecy Act in 1970.[819] The main motivation behind the passage of the Bank Secrecy Act was the pervasive tax

---

[811] Hoofnagle (2005): 5.
[812] LoPucki (2001): 94.
[813] Hoofnagle (2009).
[814] *Ibid.*
[815] Sovern, J. (2003). The Jewel of Their Souls: Preventing Identity Theft Through Loss Allocation Rules.*University of Pittsburgh Law Review*, Vol. 64 (2): 343 – 406.
[816] Hoofnagle (2009): 24.
[817] Applications can contain more than one error.
[818] *Ibid.*
[819] 31 U.S.C. Sections 5311-5330 and 12 U.S.C. Sections 1818(s), 1829(b), and 1951-1959.

evasion of (certain) citizens. Additionally, the government also introduced the Bank Secrecy Act to function as a vehicle against money laundering. Overall, the government aimed to require certain reports or records which may have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings.[820] Through the passage of the Bank Secrecy Act, the government required all domestic banks to maintain records of customer transactions and to obtain an identification number from its prospective clients. This identification number most often turned out to be a Social Security Number.[821] Furthermore, the Act also established reporting duties for financial service providers on account activity of existing clients. These include the duty for financial institutions to carry out a Currency Transaction Report (CTR)[822] whenever the institution carries out a transaction above $10,000.[823]

In part due to legal and bureaucratic challenges, the enforcement of the requirements as identified by the Bank Secrecy Act occurred at a very slow pace throughout the 1970s.[824] The legal challenges concerned the constitutionality of the Bank Secrecy Act along with disagreements and ambiguity about the definitions of 'financial institutions' and 'monetary instruments.'[825] The bureaucratic challenges proved quite diverse, but Ethan A. Nadelmann emphasizes how "...the ignorance and indifference of financial institutions to the requirements of the Bank Secrecy Act, caused in part by the government's failure to publicize them, contributed substantially to the failure in fulfilling the potential of the Act."[826]

During the following decade, the Bank Secrecy Act began to receive greater attention. The Department of the Treasury along with the Internal Revenue Service increased the enforcement and began to prosecute financial service providers for violations of the Act.[827] This may have been in response to criticism voiced by the Government Accountability Office (GAO) which emphasized in 1979 how both the Department of the Treasury along with the Internal Revenue Service needed to make more effective use of the reports as required by the Bank Secrecy Act.[828] The majority of these violations therefore focused on the reporting duties of the financial service providers rather than on the other requirement which concerned the identification of prospective clients.

---

[820] Byrne, J. (1993). The Bank Secrecy Act: Do Reporting Requirements Really Assist the Government? *Alabama Law Review*, Vol. 44: 801 – 838.

[821] Stessons, G. (2008). *Money Laundering: A New International Law Enforcement Model*. Cambridge: Cambridge University Press.

[822] 31 U.S.C. Section 5313.

[823] The threshold for the successor of the CTR, the Suspicious Activity Report (SAR) is much lower. There are two different dollar thresholds that require a SAR. They depend on the stage of discovery and the type of transaction involved. A $2,000 threshold applies if a customer is conducting or attempting to conduct a transaction(s) that aggregates to $2,000 or more. A threshold of $5,000 applies for transactions identified by issuers of money orders or traveler's checks from a review of clearance records. These thresholds are known as the $2,000 front door/$5,000 back door rule. The $2,000 front door transactions are face-to-face with the customer. The $5,000 rule applies after the records have been processed at the issuer level, thus the back door.

[824] Nadelmann, E. A. (1986). Unlaundering Dirty Money Abroad: U.S. Foreign Policy and Financial Secrecy Jurisdictions. *Inter-American Law Review*, Vol. 18: 33 0 82.

[825] *Ibid.*

[826] *Ibid*: 36.

[827] Stessens (2008).

[828] General Accounting Office (GAO) (1979). *Statement of Richard L. Fogel before the Subcommittee on General Oversight and Renegotiation House Committee on Banking, Finance and Urban Affairs on the Use of Currency and Foreign Account Reports to Detect Narcotics Traffickers*.

Despite the increased attention, the Bank Secrecy Act continued to be a source of controversy. Various sources referred to the inadequacies of law enforcement efforts to enforce the law, but also to the Act itself.[829] GAO claimed in 1981 how the Bank Secrecy Act reporting requirements failed to meet expectations.[830] Five years later, GAO concluded how the Department of the Treasury could improve the implementation of the Bank Secrecy Act.[831]

Many others call into question the effectiveness of the reporting requirements as established by the Bank Secrecy Act, including its subsequent amendments.[832] These amendments include the Comprehensive Crime Control Act of 1984, the Money Laundering Control Act of 1986, and the Anti-Drug Abuse Act of 1988. All of these amendments introduced further changes to the reporting duties as originally imposed in the Bank Secrecy Act.[833]

The most recent amendment to the Bank Secrecy Act of 1970 occurred after the events of September 11, 2001. Megan Roberts describes how "[i]n the wake of the hijackings and the massive destruction that ensued, investigators learned that some of the terrorists had fake social security numbers and had opened bank accounts."[834] The 9/11 Commission, on the other hand, refutes this claim and writes "[c]ontrary to numerous published reports, there is no evidence the hijackers ever used false Social Security Numbers to open any bank accounts. While the hijackers were not experts on the use of the U.S. financial system, nothing they did would have led the banks to suspect criminal behavior, let alone a terrorist plot to commit mass murder."[835] Even so, Roberts describes how according to estimations, the entire plot required less than $500,000 to finance. Approximately $110,000 of the money found its way into the United States via wireless transfers from Dubai and Saudi Arabia. These transfers came through Citibank in New York, which never filed a Suspicious Activity Report (SAR), despite the legal reporting duties as noted in the Banking Secrecy Act.[836]

Furthermore, Mohamed Atta, among the chief architects of the events of September 11, maintained a bank account in the United States with SunTrust and received a $70,000 wire transfer. Again, the bank failed to file a SAR. The events of September 11, 2001, especially its aftermath directly led to the passage of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act or Patriot Act). This passage occurred only weeks after September 11, 2001, in (stark) contrast to other pieces of legislation, which often consume considerable time before their enactment. This, along with its contents, led to considerable criticism

---

[829] Nadelmann (1986) mentions the General Accounting Office, Congressional committees, and internal agency auditors, among the sources who demonstrated the inadequacies.

[830] General Accounting Office (GAO) (1981). *Bank Secrecy Act Reporting Requirements Have Not Yet Met Expectations, Suggesting Need for Amendment.*

[831] General Accounting Office (GAO) (1986). *Bank Secrecy Act: Treasury Can Improve Implementation of the Act.*

[832] See for example Byrne (1993); Hughes, S. J. (1992). Policing Money Laundering Through Funds Transfers: A Critique of Regulation under the Bank Secrecy Act. *Indiana Law Journal*, Vol. 67: 283 – 330.

[833] Stessons (2008).

[834] Roberts, M. (2003). Big Brother Isn't Just Watching You, He's Also Wasting Your Tax Payer Dollars: An Analysis of the Anti-Money Laundering Provisions of the USA Patriot Act. *Rutgers Law Review*, Vol. 56: 573 – 602.

[835] National Commission on Terrorist Attacks upon the United States (2004). *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*: 237.

[836] Roberts (2003).

from various sources.[837] The Patriot Act of 2001 contained many provisions which aimed to provide law enforcement officials along with intelligence agencies the tools to deter future terrorist operations and apprehend terrorists. Part of the Patriot Act, specifically Title III, concerns the financial services industry. Title III, or rather the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, introduced various regulatory requirements for the industry which impacted several common financial transactions. Section 326 details the requirements introduced by the Act to verify the identification of consumers. The Act requires the Secretary of the Treasury to "...prescribe regulations setting forth the minimum standards for financial institutions and their customers regarding the identity of the customer that shall apply in connection with the opening of an account at a financial institution."[838] Furthermore, the Act states how "[t]he regulations shall, at a minimum, require financial institutions to implement, and customers (after being given adequate notice) to comply with, reasonable procedures for— …verifying the identity of any person seeking to open an account to the extent reasonable and practicable;…maintaining records of the information used to verify a person's identity, including name, address, and other identifying information; and…consulting lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency to determine whether a person seeking to open an account appears on any such list."[839]

As requested, the Department of the Treasury sets forth a proposed rule for the identification of prospective clients in the financial services sector. In its proposed rule, the Department states "[r]ather than imposing the same list of specific requirements on every bank, regardless of its circumstances, the proposed regulation requires all banks to implement a Customer Identification Program (CIP) that is appropriate given the bank's size, location, and type of business."[840] Further along, the Department notes its mandate to require banks to implement and subsequently comply with reasonable procedures for identity verification when prospective clients wish to open an account. The Department claims how "[t]he proposed regulation implements this requirement by providing that each bank must have risk-based procedures for verifying the identity of a customer that take into consideration the types of accounts that banks maintain, the different methods of opening accounts, and the types of identifying information available."[841] The Department only specifies a limited number of requirements with respect to the opening of accounts by prospective clients, these include "[a]t a minimum, a bank must obtain from each customer the following information prior to opening an account or adding a signatory to an account: name; address;

---

[837] See for example Breinholt, J. (2005). How about a little perspective: The USA Patriot Act and the uses and abuses of history. *Texas Review of Law & Politics*, Vol. 9: 17 - 62; Rackow, S. (2002). How the USA Patriot Act will permit governmental infringement upon the privacy of Americans in the name of "intelligence" investigations. *University of Pennsylvania Law Review*, Vol. 150: 1651 - 1696; Lilly, J. R. (2003). National Security at what price? A look into civil liberties concerns in the information age under the USA Patriot Act of 2001 and a proposed constitutional test for future legislation. *Cornell Journal of Law & Public Policy*, Vol. 12: 447 – 472.

[838] 31 U.S.C. § 5318.

[839] *Ibid.*

[840] Department of the Treasury (2003a). 31 CFR Part 103. Available at: http://www.treas.gov/press/releases/docs/staterule.pdf (last accessed July 5, 2010): 6.

[841] *Ibid.*: 7.

for individuals, date of birth; and an identification number."[842] This identification number must be a taxpayer identification number, such as a Social Security Number, individual taxpayer identification number, or an employer identification number. For non-U.S. persons, the bank must obtain an identification number, such as a taxpayer identification number; passport number and country of issuance; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard. These requirements coincide with the practices already in place at banks in the United States, as the Department of the Treasury recognizes. When this verification of identity must occur for prospective clients remains up to the financial service provider.[843]

With regard to the documents used for the verification of identities of clients, the Department of the Treasury merely mentions the usage of unexpired government issued identification which establishes the nationality or residence of the client and also bears a photograph or similar safeguard, such as another means of biometrics. Despite the relatively general requirements set forth by Treasury in the proposed rule, the Department received over 34,000 comments.[844] Based on the comments, the Department of the Treasury decided to maintain its original decisions. Treasury reconfirmed the lack of need to expressly prohibit specific foreign issued identification documents.[845] Furthermore, Treasury "…reaffirmed its original judgment that the maintenance of photocopies in all cases did not provide a security benefit that justified the additional record keeping burden."[846]

The interesting aspect of Title III of the Patriot Act is that the main provisions had been under consideration for a number of years prior to the September 11 attacks.[847] Mark E. Plotkin and B. J. Sanford reinforce this idea when they describe the political momentum generated through the aftermath of September 11.[848] The original intent to introduce the know your customer provisions date back to December 7, 1998 when the Federal Deposit Insurance Company (FDIC), along with various other agencies including the Department of the Treasury, the Federal Reserve, the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), proposed regulations which codified specific know your customer requirements. These proposed rules "…would have required each bank

---

[842] *Ibid:* 9.

[843] As the Department of the Treasury (2003a: 10) concludes, "Treasury considered proposing that a customer's identity be verified before an account is opened or within a specific time period after the account is opened. However, Treasury recognizes that such a position would be unduly burdensome for both banks and customers and therefore contrary to the plain language of the statute, which states that the procedures must be both reasonable and practicable. The amount of time it will take an institution to verify identity may depend upon the type of account opened, whether the customer is physically present when the account is opened, and the type of identifying information available."

[844] Department of the Treasury (2003b). *Fact Sheet: Results of the Notice of Inquiry on Final Regulations Implementing Customer Identity Verification Requirements under Section 326 of the USA PATRIOT Act.*

[845] The call for the prohibition of specific foreign issued identification documents might be the result of the concern over the matricula consular, which is an official identity card issued by the Mexican government. The acceptance of the matricula consular by financial service providers allows illegal immigrants to circumvent the potential suspicion over their lack of visa to reside in the United States. The Center for Immigration Studies (CIS) devoted a backgrounder to the topic. See Dinerstein, M. (2003). *IDs for Illegals: The 'Matricula Consular' Advances Mexico's Immigration Agenda*. Backgrounder, Center for Immigration Studies.

[846] Department of Treasury (2003b): 1.

[847] Plotkin, M. E. & B. J. Sanford (2006). Patriot Act: The Customer's View of "Know Your Customer"–Section 326 of the USA Patriot Act. *Bloomburg Corporate Law Journal*, Vol. 1: 671.

[848] *Ibid.*

and savings association to develop a program designed to determine the identity of its customers; determine its customers' sources of funds; determine the normal and expected transactions of its customers; monitor account activity for transactions that are inconsistent with those normal and expected transactions; and report any transactions of its customers that were determined to be suspicious in accordance with the OCC's existing suspicious activity reporting regulations."[849] The proposed regulation received fierce criticism from the financial service industry and the public. Overall, the proposed rules received over 16,000 comments during the comment period. Nearly all those who commented opposed adoption of the proposed rule. For private citizens, the opposition was based on privacy concerns. Whereas for the financial service industry, the potential administrative burden of carrying out the rule seemed to be highly unattractive. Subsequently, on March 23, 1999, the various organizations withdrew the proposed regulation.[850] The Office of the Comptroller of the Currency summarized the arguments from the banking sector as follows: "(1) the regulation would be very costly to implement, especially for small banks; (2) the Know Your Customer program would invade customer privacy; (3) commercial banks would be unfairly disadvantaged and lose customers if all segments of the financial services industry are not covered; (4) compliance with the regulation would divert resources from Y2K preparation; (5) the Agencies lack authority to adopt the regulation; (6) public confidence in the banking industry would be harmed by the regulation; and (7) the regulation is both unnecessary and redundant, as banks are already familiar with their customers and have adequate procedures in place."[851]

There are other objections posed against the implementation of know your customer requirements. These generally come from those who fear the expansion of the Federal government and its dominance in areas where State and local government ought to remain sovereign, according to their interpretation of the United States Constitution. Representative Ron Paul referred to the attempt at an introduction of know your customer requirement as an example of an interventionist approach.[852] While the Patriot Act also stumbled upon considerable resistance from the public, academics and interest groups, the political arena stood firmly behind the expansion of powers granted through the Act. The political momentum silenced any political and public resistance.

Not everyone is critical of Title III. Certain sources support its implementation. Ross Quinn Panko writes how contrary to the assertions made by critics, "...the administrative burden imposed by Title III is a reasonable extension of banks' pre-existing duties under the BSA and its due diligence provisions are consistent with international recommendations. Moreover, Title III's privacy-implicating provisions justifiably call upon customers to make a limited sacrifice of

---

[849] Office of the Comptroller of the Currency (1999). 12 CFR Part 21. Available at: http://www.occ.treas.gov/fr/fedregister/64fr15137.htm (last accessed July 5, 2010).

[850] *Ibid.*

[851] Qtd. In Plotkin & Sanford: 672.

[852] In his testimony for the Hearing on proposed 'Know Your Customer' regulations for the House of Representative Judiciary Committee, Commercial and Administrative Law Subcommittee (March 4, 1999), Ron Paul stated how "[c]onstitutionally, there are only three federal crimes. These are treason, piracy on the high seas, and counterfeiting. The federal government's role in law enforcement ought to be limited to these constitutionally federal crimes. As such, the criminal laws concerning issues other than these must, according to the ninth and tenth amendments, be reserved to state and local governments. The eighteenth and twenty-first amendments are testaments to the constitutional restrictions placed upon police power at the federal level of government."

their privacy in response to the documented dangers of poor information-sharing and inadequate customer identification verification."[853] There is merit to part of the argument set forth by Panko. Certainly the know your customer requirements set forth in the USA Patriot Act coincide with international recommendations and many aspects of the proposed rule of the Department of the Treasury overlap with requirements as identified by the Bank Secrecy Act. The implementation of the international recommendations, at least in part, in other areas of the world such as Europe surely demonstrates a stark contrast with the controversy witnessed in the United States. This returns in the following section on the Netherlands.

Overall, the above demonstrates the resistance of financial service providers to engage in increased identity verification, whether for the opening of bank accounts or the extension of individual credit via, for example, credit cards. Such increased energy and investment of resources decreases potential profits, but also leads to slower and less convenient services for consumers, which financial service providers abhor. For the government, hesitance appears to be the adjective to best describe its approach with respect to involvement in the aspect of (prospective) client identification. As a result, the application process in the United States, especially with regard to credit cards, leaves ample opportunity for perpetrators of financial identity theft. The results obtained by Hoofnagle through his study of applications of victims of financial identity theft provide empirical evidence for such assertions. Such a situation shall remain the same as long as "[m]ore money can be made by tolerating high levels of fraud than by more carefully screening against impostors. The market rewards lax authentication practices, because market actors risk losing new customers to competitors if they delay transactions to prevent fraud. Identity theft is an externality of the instant credit marketplace."[854] The endemic dilemma still dominates the application process, just as it did several decades ago.

5.2.2 The Netherlands

Identification procedures in the financial services sector began to attain political attention during the start of the 1980s. This came mainly as a result of fiscal fraud accomplished through the misuse of identification information. After the media published various stories about the usage of incorrect names by both clients and banks in 1982, banks once again brought their internal guidelines about identity determination under the attention of their employees.[855] Despite the existence and usage of internal guidelines by banks, the Lower House began to express its interest in government involvement in the identification process. Instead of specific legislation to regulate the identification process of financial services in the Netherlands, the government supported the development of a code of conduct between the representative organizations of the involved market actors and the Dutch Central Bank. This agreement came about in 1986 and maintained as its primary objective to develop a uniform code of conduct for banks in the Netherlands with respect to the methods of identity determination.[856] This code of

---

[853] Panko, R. (2004). Banking on the USA Patriot Act: An Endorsement of the Act's Use of Banks to Combat Terrorist Financing and a Response to its Critics. *SSRN Working Paper Series:* 58.
[854] Hoofnagle (2009): 35.
[855] *Kamerstukken II* 1986 – 1987, 19 904, nr. 3.
[856] *Ibid.*

conduct became a legal framework for the identification process when the government transformed the code of conduct into a general rule of administrative law in 1988.[857]

More significant involvement of the government remained absent until the international arena became engaged and began to devote attention to the topic of the identification process in the financial services sector. The topic of client identification in the financial services sector became a political issue on an international level in light of the increased attention devoted to money laundering. The Basel Committee emphasized the importance of client identification in the financial services sector in 1988 through its publication of *The Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering*. In the paper, the Basel Committee "…stipulates the basic ethical principles and encourages banks to put in place effective procedures to identify customers, decline suspicious transactions and cooperate with law enforcement agencies."[858] During the yearly summit meeting between the G7 and the European Commission in 1989, officials decided to introduce a Task Force. This Financial Action Task Force was to include Summit Participants and other countries interested in these problems. The mandate of the intended Task Force was to "…assess the results of cooperation already undertaken in order to prevent the utilization of the banking system and financial institutions for the purpose of money laundering, and to consider additional preventive efforts in the field, including the adaption of the legal and regulatory systems so as to enhance multilateral judicial assistance."[859] The first report of the Financial Action Task Force was to be published by April 1990, but actually came out on February 6, 1990.[860] The report focuses on the role of financial institutions in connection to money laundering and also returns to this role in its recommendations. The forty recommendations provided by the FATF are divided into four categories.

The most relevant of the four is enhancement of the role of the financial system. More specifically, the FATF provides recommendations which focus on customer identification and record keeping rules. The FATF provides the following three recommendations within this category. First, the FATF states "[f]inancial institutions should not keep anonymous accounts or accounts in obviously fictitious names: they should be required (by law, by regulations, by agreements between supervisory authorities and financial institutions or by self-regulatory agreements among financial institutions) to identify, on the basis of an official or other reliable identifying document, and record the identity of their clients, either occasional or usual, when establishing business relations or conducting transactions (in particular opening of accounts or passbooks, entering into fiduciary transactions, renting of safe deposit boxes, performing large cash transactions)."[861]

Secondly, the FATF states "[f]inancial institutions should take reasonable measures to obtain information about the true identity of the persons on whose

---

[857] *Kamerstukken II* 1992 – 1993, 23 008, nr. 3.
[858] Basel Committee on Banking Supervision (2001). *Customer due diligence for banks*.
[859] Qtd. In Mul, V. (1999). *Banken en witwassen*. Sanders Instituut: Gouda Quint: 105.
[860] Financial Action Task Force (FATF) (1990). *The Forty Recommendations of the Financial Action Task Force on Money Laundering*.
[861] *Ibid:* 2.

behalf an account is opened or a transaction conducted if there are any doubts as to whether these clients or customers are not acting on their own behalf..."[862]

Third, "[f]inancial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour. Financial institutions should keep records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the account is closed. These documents should be available to domestic competent authorities in the context of relevant criminal prosecutions and investigations."[863]

The last recommendation specifically aims to develop a paper trail which assists in the fight against money laundering. The first two, on the other hand, specifically focus on the identification of the prospective client during the application process.

The curious aspect about this approach to money laundering is how the emphasis placed on the correct identification of the client also places a premium on identities themselves. For such requirements increase the necessity for those involved in money laundering practices to misuse the identity of another person in an effort to prevent potential repercussions. As a result the recommendations set forth could potentially lead to a displacement of the problem through the commitment of identity related crime in an effort to accomplish the money laundering objective. As the definition provided by Koops & Leenes in chapter 2 stated, identity theft occurs through the commitment of an unlawful activity whereby the identity of an existing person is used as a principal tool or target. Identity becomes a principal tool for perpetrators of money laundering to circumvent the requirements provided through the anti-money laundering framework. The evolution of money mules (see chapter 7) appears to support this notion.

The recommendations set forth by the FATF specifically geared toward the identification process of clients in the financial services sector became the foundation for the on June 10, 1991, introduced European Union Directive on prevention of the use of the financial system for the purpose of money laundering.[864] The Directive incorporated the recommendations introduced by the FATF and required Member States to "…ensure that credit and financial institutions require identification of their customers by means of supporting evidence when entering into business relations, particularly when opening an account or savings accounts, or when offering safe custody facilities."[865]

The existing legal framework in the Netherlands as officially established in 1988 proved, despite good compliance in practice, insufficient in light of the Directive.[866] The government deemed an intensification of the identification process within the financial services sector of the essence especially in response to

---

[862] *Ibid.*
[863] *Ibid.*
[864] Council Directive 91/308/EEC.
[865] *Ibid.*
[866] *Kamerstukken II* 1992 – 1993, 23 008, nr. 3.

the Directive. As a result of such intensification, it was unfeasible to maintain the principle of self-regulation. Self-regulation needed to move aside for a stricter legal framework with broad applicability.[867] Whereas the code of conduct used for several years in the Netherlands primarily focused on the fight against fiscal fraud, the stricter legal framework needed to focus on both money laundering and fiscal fraud. This expanded the scope of applicability. Part of the implementation occurred through the Identification for Financial Services Act[868] which officially became enacted in 1994.[869] This law specifically requires financial service providers to determine and verify the identity of a client before the client receives the financial service from the provider. Such identification must occur through the acceptance of a valid identification document. These identification documents must be one of the following: a travel document, such as a passport or national identification card, a driver's license, or an immigration document which demonstrates the legal right to reside in the Netherlands.

The other aspect of the Directive which focused on the due diligence recommendations as provided by the FATF developed into another law which described the requirements for notification with respect to unusual transactions. Interesting to note is how the Netherlands is different in its formulation of unusual transactions as opposed to suspicious transactions. The concept of unusual transactions is derived from the FATF as opposed to the Directive which refers to suspicious transactions. According to Stessons, "[t]he Dutch model reflects a vision that the sifting of suspicious transactions is a law enforcement task which should be carried out by the government and not by private (financial) institutions."[870]

The implementation of the Directive by the Dutch government into two laws was a conscious choice. This choice was based on the fact that the Identification for Financial Services Act was an expansion of an existing framework, whereas the notification duty was an entirely new phenomenon.[871] Moreover, the Identification for Financial Services Act maintained two distinct goals, money laundering and fiscal fraud, which meant the law went beyond the Directive's exclusive focus on money laundering. As a result, the government determined it best to introduce two separate pieces of legislation which together composed the legislative framework in the fight against money laundering.[872]

The existing framework became the topic of additional discussion after the events of September 11, 2001. The issue of terrorist financing proved an impetus for the FATF to issue nine additional recommendations in October 2001. These nine recommendations complemented the previously published forty recommendations which specifically focused on money laundering.[873] The nine recommendations issued in 2001 aimed to provide assistance in the fight against terrorist financing and focused on, among other things, freezing and confiscating terrorist assets, and reporting suspicious transactions related to terrorism. Also in 2001, the European Union introduced its second anti-money laundering initiative

---

[867] *Ibid.*
[868] *Stb.* 1993, 604.
[869] Later the Act came to be known as the Identification for Services Act or the *Wet Identificatie bij dienstverlening*, since other types of organizations became obligated to follow the same law.
[870] Stessons (2008): 170
[871] *Kamerstukken II* 1992 – 1993, 23 008, nr. 3: 3.
[872] *Kamerstukken II* 2007 – 2008, 31 238, nr. 3.
[873] FATF IX Special Recommendations (2001, Amended in 2004).

which amended Council Directive 91/308/EEC.[874] The original Directive exclusively focused on the laundering of proceeds from drug related offenses but the amended version notes how there should be a wider range of predicate offenses to be included. Moreover, the Directive acknowledges how the intensified fight by the financial services sector against money laundering has led to a potential displacement of offenders to launder their proceeds via other organizations outside of the financial services sector. The Directive specifically refers to, among others, notaries, independent legal professionals, real estate agents, and casinos.[875] This expansion of applicable parties led the government in the Netherlands to amend the Identification for Services Act and the Law for reporting unusual transactions in 2003.

The introduction of the second Directive on money laundering in 2001 might lead one to conclude how this Directive proved a response to terrorist financing much the same as the additional nine recommendations issued by the FATF. This is, however, incorrect. Several years later, in 2005, the European Union issued its third directive in the fight against money laundering which also expanded the fight to include terrorist financing.[876] This was the actual response to the various terrorist events, both inside and outside of the European Union.

Besides including the issue of terrorist financing in its prevention efforts, the Directive also introduced important changes in its approach to client identification processes. As stated in the Directive, "[i]t should be recognised that the risk of money laundering and terrorist financing is not the same in every case. In line with a risk-based approach, the principle should be introduced into Community legislation that simplified customer due diligence is allowed in appropriate cases."[877] Moreover, the Directive also notes how "[c]ommunity legislation should recognise that certain situations present a greater risk of money laundering or terrorist financing. Although the identity and business profile of all customers should be established, there are cases where particularly rigorous customer identification and verification procedures are required."[878]

All of these developments at the European level logically influenced the legal landscape in the Netherlands. Especially the introduction of the third directive required amendments to the existing legislative framework. Due to the need for amendments, the Ministry of Finance expressed a desire to determine how financial service providers and other relevant corporations dealt with the available legislation. To achieve such an assessment the Ministry of Finance commissioned a study in 2006.[879]

The risk based approach developed through the third EU Directive on money laundering requires relevant organizations, including financial service providers, to develop a framework which identifies risk indicators. This framework takes into consideration client as well as service or product aspects which influence the risk assessment. When such a framework determines a low risk, organizations can use more simplified means of identification and identity verification. The supervisory organs, namely the Dutch Central Bank, can play a role when organizations require more assistance. The original law for identification of service provision

---

[874] Directive 2001/97/EC.
[875] *Ibid.*
[876] Directive 2005/60/EC.
[877] *Ibid*, L 309/17.
[878] *Ibid.*
[879] KPMG (2006). *Ontvangen signalen voor een efficiënte identificatie*. Report to the Ministry of Finances.

carried a rule based approach, which, according to respondents of the study, led to unnecessary administrative burdens.[880] Such a rule based approach also prevents a much desired flexibility. The interviews conducted by KPMG demonstrate how a majority of the respondents favor a risk based approach since such an approach affords them the flexibility to develop procedures according to the risk of the client, the service, and the institution. Smaller organizations, on the other hand, indicated a preference for clarity and specificity in the requirements set out by the government for identification procedures. For them, a uniform method is more cost effective and also more manageable.[881]

The risk based approach set forth by the European Union demonstrates its comparable nature to the emphasis placed on a risk based approach by the Department of the Treasury as described above. The implementation of the risk based approach as introduced through the third directive occurred as part of a package deal, which is a rarity in Dutch legislative history. The existence of two separate laws which together composed the core of the legislative framework to combat money laundering led to practical problems.[882] The working group on both laws set forth a recommendation to join both acts together in an effort to enhance clarity. As a result, the government decided to take the opportunity during the implementation stage of the third EU Directive to combine both the Identification for Services and Reporting Unusual Transactions Act[883] into a single piece of legislation. Together they became the prevention of money laundering and financing terrorism act.[884]

The Act requires service providers to identify the client and verify her identity. Moreover, the Act emphasizes the need to verify the identity of the ultimate recipient of the service. The third EU Directive also required member states to appoint a supervisory administrative body to ensure compliance with the legal mandate. Along with the joining of the two previous laws, the government also appointed the Dutch Central Bank as the compliance supervisor.[885] In addition, Article 27 of the law also makes incompliance with the legal requirements sanctionable through a fine.

In contrast to the United States, the aspect of client identification appears less controversial. And the changes in the legal landscape overshadow the original conclusion set forth based on the code of conduct which demonstrates how there was generally good compliance by financial service providers in the Netherlands.

Limited controversy began when in 2005 banks in the Netherlands began to send out letters to their existing clients and required them to visit the bank in order to provide them with a copy of their identification document, namely their passport or driver's license, or to send a watermarked copy. Banks claimed this was a legal mandate set forth through the Identification for Services Act, which requires identity verification and proof for the Dutch Central Bank to demonstrate such verification took place. The banks who requested a personal visit therefore also made a digital copy of the identification document. The claim, however, was misleading as the requirement for a copy of the passport was merely one interpretation of the law; it was not an explicit mandate. The Minister of Finances

---

[880] *Ibid.*
[881] *Ibid:* 20.
[882] *Kamerstukken II* 2007 – 2008, 31 238, nr. 3.
[883] *Stb.* 1993, 705.
[884] *Stb.* 2008, 303.
[885] Article 24.

along with the Dutch Central Bank decided the method used by the banks to verify the identity of existing clients was not unlawful. To remove the ambiguity surrounding the banks' actions, the Minister of Finances decided to incorporate the method as part of the law.[886]

Through the introduction of the prevention of money laundering and financing terrorism act, the government removed the fiscal obligation to maintain a copy of the identification document by financial service providers. The Act instead requires financial service providers to obtain and store the information maintained on the identification document. In particular the Act requires the service providers to store the following information once the service provider has identified and verified the identity of the client: name, date of birth, address, and the city of residence. Even so, the Act still provides financial service providers with the opportunity to request a copy of an identification document since the Act states "…or a copy of a document which contains a personal identification number and was used for identification of the client."[887]

In the Netherlands, only anecdotal evidence appears to be available about errors committed by financial service providers during the application process.[888] Banks resist the release of information about how such incidents occur, but in light of good compliance there is reason to believe such incidents of financial identity theft most likely occur through look-alike fraud or falsified identification documents. As a result, there is a certain dependency of financial service providers on the government as provider. For the quality of both the documents and the issuance process also influence the identification of (prospective) clients.

5.3 Consumer Reporting Agencies

5.3.1 United States

The introduction of consumer reporting agencies into contemporary society occurred as a result of the need for an institutional response to information asymmetry.[889] Consumer reporting agencies are a strange species in society, in particular in the United States. Historically, their internal operations carry an air of secrecy; especially the administrative records and internal correspondence remain inaccessible to outside sources. Josh Lauer notes how "[t]he history of consumer credit reporting is hampered by a lack of primary source material; there are no public archives or obvious concentrations of documentary evidence to consult."[890] According to Lauer, consumer reporting agencies deliberately remained out of

---

[886] Dekker, G. (2007). Zalm drukt digitale 'kopie paspoort' door. *Volkskrant*. Available at: http://www.volkskrant.nl/economie/article390331.ece/Zalm_drukt_digitale_kopie_paspoort_door (last accessed July 13, 2010).

[887] Article 33 part 1.

[888] The chain director of the consumer complaint center briefly referred to bank accounts opened in the name of victims (Interview, March 29, 2010, Amstelveen). This proved to be an occasional complaint, rather than a recurring phenomenon (personal communication April 12, 2010). The victim generally found out through a notification of the bank.

[889] Olegario, R. (2001). Credit-Reporting Agencies: Their Historical Roots, Current Status, and Role in Market Development. Paper presented at the World Bank workshop *The Role of Credit Reporting Systems in the International Economy*, Washington DC. Available at: http://siteresources.worldbank.org/INTWDRS/Resources/477365-1257315064764/2429_olegario.pdf (last accessed July 5, 2010).

[890] Lauer, J. (2008). *The Good Consumer: Credit Reporting and the Invention of Financial Identity in the United States, 1840-1940*. PhD Dissertation, University of Pennsylvania: 11.

sight to avoid legal action and public condemnation. Lauer managed to trace the roots of consumer reporting agencies back to New York where during the 1870s the first consumer credit reporting organizations emerged. These organizations began to spread throughout the country during the following decades. Lauer describes how individuals generally applied for a line of credit in two ways. The customer could apply directly or request, upon checkout, that the items be charged. Either way, the sales associate needed to refer the customer to the credit or office manager. "Here," writes Lauer, "the social nature of credit reached a moment of high drama. Credit, after all, is a measure of social trust. Thus to have one's creditworthiness subjected to judgment is no small matter; it is a referendum on one's morality and social standing. To be refused implies that one is undeserving, deficient, suspect."[891] The moral weight associated with the credit worthiness of an individual is a reflection of the role credit plays in society, at least in the United States. The President of the National Association proclaimed in 1918 how the industry needed to "...preach the doctrine that credit is character, and that a person who willfully abuses his credit and refuses to heed the warning must become an outcast in the business and the social world."[892]

As private sector initiatives, consumer reporting agencies developed without government involvement. Rowena Olegario described how consumer reporting agencies evolved as a result of inter-firm competition.[893] For years, consumer reporting agencies remained local independently-owned businesses until the late 1970s when computerization and consolidation, at least for nationwide consumer reporting agencies, reduced the number of nationwide corporations to three.[894] These three dominant firms, TransUnion, Equifax, and TRW still exist today, although TRW is now Experian.

Several years before the consolidation of nationwide agencies, critical accounts of consumer reporting and its associated activities began to surface, especially in relation to the potential privacy intrusions. The usual suspects of critical accounts included among others Arthur R. Miller and Alan F. Westin. Besides the critical accounts of prominent scholars in the field, the United States Congress also opened its eyes. Albeit years later. Robert M. McNamara describes how "[d]uring the period of their phenomenal growth, credit bureaus have somehow escaped the focus of both state and federal inquiry and regulation in spite of the existence of serious abuses."[895] This left consumers unprotected since common law remedies proved absent for the harms caused by the consumer reporting industry. The business practices of consumer reporting agencies introduced a plethora of problems, which required legislative involvement. G. Allan Van Fleet summarizes the problems associated with consumer reporting as follows "[i]n addition to the questionable relevancy of some of the information contained in consumer reports, attacks have been leveled at the promiscuous dissemination of an individual's files without his knowledge, let alone his consent, and at the practice of some bureaus of attempting to collect bills by threatening to ruin the debtor's credit rating."[896]

---

[891] *Ibid:* 166.
[892] Qtd. in *Ibid:* 208.
[893] Olegario (2001).
[894] A fourth, Innovus, joined the 'club' at a later stage.
[895] McNamara, R. M. (1973). The Fair Credit Reporting Act: A Legislative Overview. *Journal of Public Law*, Vol. 22: 71.
[896] Van Fleet, G. A. (1976). Judicial Construction of the Federal Credit Reporting Act: Scope and Civil Liability. *Columbia Law Review*, Vol. 76 (3): 460.

Mike Wallace and Westin conducted experiments to unravel the process through which consumer reporting agencies issued credit reports.[897] This happened, as demonstrated through the experiments, with considerable ease and indicated how anyone, regardless of purpose, could obtain the credit reports of other people. The other main problem concerned the adoption of erroneous information as part of the individual's credit report, which subsequently caused problems when the individual tried to obtain a loan, apply for a job, etc.

Despite the obvious problems caused by the consumer reporting industry, for forty years only one state considered the issue important enough to introduce legislation to regulate the industry.[898] Ironically, the business practices of the consumer reporting industry became a topic of political discussion during the consideration of the introduction of a national data bank. To make record-keeping more efficient and economical, the Bureau of the Budget commissioned a feasibility study in 1961 for the centralization and computerization of all personal records maintained by the Federal government and its agencies.[899] Several studies supported the establishment of a Federal Data Center. The potential for privacy invasions as a result of such an establishment also received attention from the Special Subcommittee on the Invasion of Privacy of the House Committee on Government Operations, which held various public hearings. The Special subcommittee published its findings, conclusions, and recommendations in 'Privacy and the National Data Bank Concept.' In the report, members of the Special Subcommittee express considerable concern about the potential harm inflicted on the privacy of individuals as a result of a National Data Bank.[900] The proposal for a National Data Bank died in Committee. During the debate about the introduction of such a public data bank, the United States Congress finally became aware of the existence of a private data bank – the consumer reporting agencies.[901]

Months before the death of the idea of a National Data Bank, a particular Member of Congress already noted the problems associated with the consumer reporting industry. Clement J. Zablocki, a Representative from Wisconsin, introduced the first 'Fair Credit Reporting Bill' after he received a complaint from a constituent. Rita B. Collins wrote the Wisconsin Representative on September 6, 1967.[902] In her letter, she described how she had been turned down for a car loan because the consumer reporting agency provided the car dealer with erroneous information. Specifically, the credit report stated how Collins and her husband owed money to a trucking firm. In response to the letter, Zablocki introduced his bill which would grant individuals the right to know the identity of the consumer reporting agency, the contents of the report, and, in the case of an adverse report, the specific facts or allegations upon which the report was based. Zablocki's bill never escaped Committee discussions, but still served a vital function as a source of inspiration for similar proposals and significant congressional concern about the issue. Consumer reporting agencies no longer managed to escape the attention of Congress and on March 12, 1968 the Subcommittee on the Invasion of Privacy commenced its hearings on the industry. These hearings became known as the

---

[897] McNamara (1973).
[898] *Ibid.*
[899] *Ibid.*
[900] *Ibid.*
[901] *Ibid.*
[902] *Ibid.*

Gallagher hearings. According to McNamara, "[t]he Gallagher hearings were the cumulative result of the awareness of the problem caused by the work and the study done on the National Data Bank and the thousands of letters and reports of cases received by Gallagher."[903]

Upon Gallagher's recommendation, the consumer reporting industry gathered to develop guidelines for self-regulation. These guidelines, submitted to the Committee by the industry, received positive feedback from Gallagher. As a result of the guidelines, Gallagher considered further legislation unnecessary. McNamara describes how the development of the guidelines fulfilled a political strategy for the consumer reporting industry. Regulation was in the air and self-imposed guidelines proved to be the lesser of two evils. Self-imposed guidelines carried an air of industrial ethics and concern. But, as McNamara notes, "[b]eneath this 'good industry facade,' however, was the more subtle benefit, namely, that self-regulation would impose no legal duties."[904] Further along in his overview, McNamara reiterates how "[f]acades of concern and statements of sincerity may abate criticism but are easily seen for what they are by investigating daily business practices."[905] Despite the praise expressed by Gallagher, the self-imposed guidelines failed to appease other Members of Congress.

Senator Proxmire introduced his version of the 'Fair Credit Reporting Bill' only two and a half weeks after the industry proposed its guidelines. Gallagher, as an industry champion, presented the guidelines to Congress in hopes of avoiding legislation. Proxmire again emphasized the uselessness of the guidelines with respect to the industry problems and began to hold hearings on S. 823, the Fair Credit Reporting Bill, on May 23, 1969. His hearings increased the public and political attention on the issue, mainly through the repetition of earlier problems identified about the consumer reporting industry. McNamara eloquently exposes the politics of the public policy process when he describes how after S. 823 passed in the Senate, the House of Representative referred the bill to the House Committee on Banking and Currency, where "...it was to be stalled for many months."[906] "One of the possible reasons for the apparent lethargy of the House Committee", according to McNamara, "was its self-interest in holding hearings on an alternate bill submitted by Congresswoman Leonore Sullivan which she had titled the 'Good Name Protection Bill.'"[907] Whereas the Good Name Protection Bill died a quiet death in Committee, the Fair Credit Reporting Bill moved along and ultimately found itself signed into law on October 26, 1970.

The Fair Credit Reporting Act (FCRA) states that "…it is the purpose of this subchapter to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this subchapter."[908] The FCRA defines the permissible purposes of consumer reports and the circumstances under which consumer reporting agencies may furnish

---

[903] *Ibid.*
[904] *Ibid.*
[905] *Ibid:* 86.
[906] *Ibid*.
[907] *Ibid:* 97.
[908] Fair Credit Reporting Act 15U.S.C. § 1681. Congressional findings and statement of purpose.

credit reports to third parties.[909] The FCRA also grants consumers the right to receive a copy of their credit report.[910] In addition, the FCRA prohibits the inclusion of obsolete information as part of the credit report but also limits liability of consumer reporting agencies.

The FCRA has been subject to severe criticism, especially since the industry appeared to maintain significant influence on its ultimate formulation. Arthur Miller captures the importance of the industry's influence when he writes, "[t]he original Proxmire bill had been butchered; it was drawn and quartered and its vitals were left on the Committee's chopping block. How that came to pass is no mystery. Industry lobbyists and bank-oriented senators engaged in the dissection, while advocates of consumer protection quietly relied on the legislative process to produce a bill that would respond to the needs of the public."[911] James B. Rule claims the FCRA is part of a tradition, which he labels as "the genius of American liberalism." "It is the genius of American liberalism," Rule writes, "that, when faced with a particularly unconscionable practice by some powerful interest, it regulates that interest in such a way as both to mitigate the sting of the abuse and at the same time to consolidate the position of the perpetrators."[912]

Even so, others recognize the FCRA's value and provide the Act with numerous positive labels. The FCRA is seen as the first 'breakthrough[913], 'a truly significant beginning'[914] and 'a major first step.'[915] These positive responses, on the other hand, also recognize the need for more work and as such are best categorized as constructive criticism.

Many years later, others still applaud the Act. Fred H. Cate *et al.* state "[f]or more than 30 years, the Fair Credit Reporting Act has deftly regulated the U.S. credit reporting system. The product of extensive congressional hearings, the Act creates a simple, powerful, and largely self-enforcing regulatory structure. It has proven so efficient, flexible, and durable that, with only a single substantive amendment, it has guided the world's most robust credit reporting system and overseen exceptional growth in consumer mortgages and other credit opportunities for three decades."[916]

The industry itself emphasized the success of the FCRA when new potential legislation featured on the horizon. Lawrence D. Frenzel describes how "[t]he consumer reporting agencies have consistently, adamantly, and unanimously maintained that the FCRA is overwhelmingly successful in fulfilling Congress' express intent. Armed with statistics revealing extremely small numbers of consumer complaints–compared to the millions of consumer reports issued—the reporting agencies contend that the casualties of consumer reporting abuses are negligible."[917] Frenzel describes furthermore how consumer reporting agencies

---

[909] 15 U.S.C. § 1681b.
[910] 15 U.S.C. § 1681g.
[911] Qtd. In Van Fleet (1976): 465.
[912] Rule (1974): 214.
[913] Ullman, C. M. (1972). Liability of Credit Bureaus after the Fair Credit Reporting Act: The Need for Further Reform. *Villanova Law Review*, Vol. 17: 44 – 72.
[914] Feldman, S. (1974). The Fair Credit Reporting Act—From the Regulators Vantage Point. *Santa Clara Lawyer*, Vol. 14: 459 – 490.
[915] Frenzel, L. D. (1977). Fair Credit Reporting Act: The Case for Revision. *Loyola of Los Angeles Law Review*, Vol. 10: 409 – 439.
[916] Cate, F. H., Litan, R. E., Staten, M. & P. Wallison (2003). *Financial Privacy, Consumer Prosperity, and the Public Good: Maintaining the Balance*. Washington, DC: American Enterprise Institute Press (AEI): 1.
[917] Frenzel (1977): 414.

claim consumer complaints are a result of consumers being disgruntled over denied benefits rather than having legitimate grievances toward the consumer reporting agency. Ironically, "[t]hese arguments tend to exculpate the consumer reporters from responsibility for consumer complaints, and place the blame on the consumers themselves."[918] An approach which carries a flavor of familiarity throughout the more general problem of identity theft, as will especially become evident in chapter 6. Frenzel describes how "[u]nder close analysis, the arguments supplied by the information merchants are illusory; they are merely a clever alchemization of quantitative data into qualitative conclusions."[919]

Proxmire returned in 1973 in an effort to revive his original efforts. In part based on the recommendations set forth by the Federal Trade Commission (FTC), Proxmire set forth Senate Bill 2360. According to Proxmire, "[o]ne of the most significant provisions of S. 2360 would entitle consumers to physically inspect their credit file and to receive a written copy of all the information in the file. The present law requires only an oral disclosure and has led to a number of consumer complaints and misunderstandings."[920] Another important provision proposed through S. 2360 was an increased responsibility on the 'user' of consumer credit information with regard to informing consumers about the reasons why they were rejected credit by the 'user.' S. 2360 specifically requires credit providers to tell consumers in writing the specific reasons for the rejection of credit and they must also provide consumers with a copy of any credit report.

The hearings illustrate the resistance expressed by the industry toward the proposed amendments to the FCRA. The statement provided by John L. Spafford captures the industry's aversion to increased consumer rights. "Mr. Chairman," Spafford stated, "…to put it mildly, the reaction of our membership to some of your proposed changes in the FCRA has been one of shock over the severity of the proposals. Our members are dismayed that…this industry is now faced with some proposals which were discarded after careful study 3 years ago, and new ones which would raise costs and seriously hamper the effectiveness of consumer reporting agencies."[921] The discarded aspects Spafford refers to are perhaps not the result of 'careful study' but rather the impact of powerful lobbying capacity from the industry which managed to influence the ultimate provisions in the FCRA. With respect to the requirement for credit providers to specifically state the reasons for credit rejection, Spafford states "[a]lthough ACB defends the credit grantor's right to make a decision without having to identify specific items of information that caused a decline, it is true that the present 615 (a) requirement has in some cases made the credit bureau the 'whipping boy' for credit grantors who are too broad and general in their explanation of why credit could not be extended."[922]

Even so, Spafford expressed his preference for an alternative route and described the industry's attempt to persuade credit grantors to use a multiple choice decline letter. Spafford believed the industry deserved more time to

---

[918] *Ibid:* 415.
[919] *Ibid:* 416.
[920] Proxmire, W. (1973) Opening statement to the U.S. Senate Subcommittee on Consumer Credit of the Committee on Banking, Housing and Urban Affairs. *Fair Credit Reporting Act—1973*, Hearing, October 1, 1973: 3.
[921] Spafford, J. L. (1973). Testimony to the U.S. Senate Subcommittee on Consumer Credit of the Committee on Banking, Housing and Urban Affairs. *Fair Credit Reporting Act—1973*, Hearing, October 1, 1973: 15.
[922] *Ibid:* 18.

encourage credit grantors to recommend the use of such a letter, which was developed by the FTC with the assistance of ABC. Richard M. Davis is more forthright about his support for the provision which provides consumers with specific reasons as to the rejection of their application for credit. As he stated, "[w]e agree that more specific reasons for denial of credit would provide many benefits for the consumer and the system. ICBM would like to go on record as seeking to protect consumers, and their right to know why they are specifically refused credit."[923] Those directly implicated to provide specific reasons for rejection proved averse against such a legal requirement.[924]

Others before the Subcommittee supported the resistance against the 'radical changes' proposed by Proxmire. W. Lee Burge, President of the Retail Credit Co., believed the amendments introduced were neither needed nor justified. He also states how, "[m]ost of the changes now proposed were debated and specifically rejected by the responsible subcommittee and the full committee in 1969, and by the conference committee in 1970."[925]

Once again, the lobbying capacity of the industry proved fierce and effective. Significant changes to the FCRA failed to come about until several decades later when the United States Congress passed the Fair and Accurate Credit Transactions Act (FACTA) in 2003. The primary aim of FACTA is to provide amendments to the FCRA which aspire "...to prevent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer records, make improvements in the use of, and consumer access to, credit information, and for other purposes."[926] Most importantly, FACTA establishes the need for red flag guidelines and requires the Federal Banking Agencies, the National Credit Union Administration, and the Federal Trade Commission to jointly issue such guidelines.[927] Basically, FACTA requires the Agencies to identify patterns,

---

[923] Davis, R. M. (1973). Testimony to the U.S. Senate Subcommittee on Consumer Credit of the Committee on Banking, Housing and Urban Affairs. *Fair Credit Reporting Act—1973*, Hearing, October 1, 1973: 178.

[924] Bernard C. Gilbert (1973: 209) stated during the hearing, "[i]nsofar as retailers are concerned the requirement that the user provide the consumer a reason for credit denial has transcended the boundaries of credit reporting and vaulted into the arena of credit granting. In reviewing this proposed requirement one is struck with the notion that the retailer is being forced to justify his credit-granting procedures. The opportunity to purchase goods on credit appears to be treated as a right rather than something which must be earned and which is inevitably based on the judgment of the credit grantor."

[925] Burge, W. L. (1973). Testimony to the U.S. Senate Subcommittee on Consumer Credit of the Committee on Banking, Housing and Urban Affairs. *Fair Credit Reporting Act—1973*, Hearing, October 1, 1973: 59.

[926] Fair and Accurate Credit Transactions Act of 2003. Pub. L. No. 108-159.

[927] More specifically, FACTA requires these institutions to "…establish and maintain guidelines for use by each financial institution and each creditor regarding identity theft with respect to account holders at, or customers of, such entities, and update such guidelines as often as necessary; prescribe regulations requiring each financial institution and each creditor to establish reasonable policies and procedures for implementing the guidelines established pursuant to subparagraph (A), to identify possible risks to account holders or customers or to the safety and soundness of the institution or customers; and prescribe regulations applicable to card issuers to ensure that, if a card issuer receives notification of a change of address for an existing account, and within a short period of time (during at least the first 30 days after such notification is received) receives a request for an additional or replacement card for the same account, the card issuer may not issue the additional or replacement card, unless the card issuer, in accordance with reasonable policies and procedures— notifies the cardholder of the request at the former address of the cardholder and provides to the cardholder a means of promptly reporting incorrect address changes; notifies the cardholder of the request by such other means of communication as the cardholder and the card issuer previously agreed to; or uses other means of assessing the validity of the change of address, in accordance with reasonable policies

practices, and specific forms of activity which possibly indicate the existence of identity theft. The development of such guidelines concern financial service providers in general rather than consumer reporting agencies in particular. This section or the discussion of FACTA also applies to other business practices discussed throughout the chapter.

The proposed guidelines of the Agencies which became available for public commentary received criticism from consumer advocates. The Agencies described how consumer advocates complained about the proposed regulations which "…provided too much discretion to financial institutions and creditors to decide which accounts and Red Flags to include in their Programs and how to respond to those Red Flags. These commentators stated that the flexible and risk-based approach taken in the proposed rulemaking would permit 'business as usual.'"[928] Interestingly, certain small financial institutions expressed similar concerns about the flexibility afforded through the proposed guidelines. They called upon the Agencies to provide more clarity and more structure as part of their guidelines.[929]

Most commentators, on the other hand, criticized the Agencies for the overly prescriptive nature of the proposal. Many of these commentators included financial service providers who claimed the requirements set forth by the proposal surpassed the requirements as mandated by FACTA. Furthermore, those critical of the proposal also seemed concerned about the costs involved and claimed how the proposal would complicate existing efforts to detect and prevent identity theft. Certain businesses even claimed "...the rulemaking was unnecessary because large businesses, such as banks and telecommunications companies, already are motivated to prevent identity theft and other forms of fraud in order to limit their own financial losses."[930] Additionally, a few financial service providers claimed the primary cause of identity theft was the lack of care on the part of consumers. These financial service providers asserted that consumers themselves should be held responsible for the protection of their identifying information. The overview of comments received demonstrates the inherent conflict of interest present among and between actors, both inside and outside of the private sector.

The Red Flags Rule published by the Agencies requires certain businesses and organizations to develop, implement, and administer identity theft prevention programs. The program must include four basic elements which together compose a framework to address the threat of identity theft. First, the program introduced by the organization must include reasonable policies and procedures which can identify red flags. Second, the program must be able to detect the red flags which the organization previously identified. The third element requires the organization to specify appropriate actions which the organization needs to take to address the red flags. And the fourth aspect requires organizations to adopt means of evaluation as part of their program, especially since identity theft is a continuously evolving threat and new risks arise as time passes.[931]

---

and procedures established by the card issuer in accordance with the regulations prescribed under subparagraph (B)."

[928] Office of the Comptroller of the Currency (2007). 12 CFR Part 41. Available at: http://www.occ.gov/ftp/release/2007-122a.pdf (last accessed July 5, 2010).

[929] *Ibid.*

[930] *Ibid:* 7–8.

[931] Federal Trade Commission (FTC) (n.d.). Fighting Fraud with the Red Flags Rule: a How-to Guide for Businesses. Available at http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf

To make these four core aspects more concrete, the FTC provides examples for organizations. For the first step, the FTC describes the following possible red flags: alerts, notifications, or warnings from consumer reporting agencies. In this sense, the consumer reporting agencies play a crucial role in the realm of situational crime prevention. For as an intermediary, they maintain information about consumers and victims which can potentially prevent additional or future victimization. This aspect is, however, not entirely the responsibility of consumer reporting agencies, since the provision of alerts, notifications, and warnings also requires financial service providers to adhere to such red flags in an effort to accomplish the prevention of financial identity theft. Moreover, the FTC also refers to the potential for red flags with regard to suspicious documents, personal identifying information, or account activity.[932] For detection, the FTC distinguishes between new and existing accounts. Especially since both are subject to different types of 'attacks.'

The actual implementation of the red flags guidelines remain a subject of continuous postponement. The original date of compliance was November 1, 2008. Since many organizations impacted by the guidelines proved ill-prepared for the necessary preparations, the FTC moved the deadline to May 1, 2009.[933] The compliance data continued to be a subject of negotiation and the FTC extended the deadline to November 1, 2009 before offering another extension to move the date of compliance to June 1, 2010.[934] This date was once again changed and the most recent date of compliance is December 31, 2010. As a result, the red flags rule is yet to go into effect and as such it is difficult to assess its impact on the prevalence of financial identity theft.[935]

But the actual effectiveness from the red flags is embedded in both the detection of such flags and the response to such detection. As Hoofnagle concluded, "[a]utomated fraud detection systems at the consumer reporting agencies indicated that fraud could be present in 3 of the 4 mortgage applications in X5's file. One warned, 'Substantial difference between address submitted in credit request and addresses in credit file.' Two of these red flag warnings indicated that the applicant/impostor's DOB did not match X5's. It is unclear what steps the creditor grantor took to resolve these red flags before extending mortgages to the impostor."[936]

Overall, consumer reporting agencies maintain different functions in the facilitation of financial identity theft. The release of credit reports to third parties, especially financial service providers, is an essential aspect of the credit granting process. In this regard, consumer reporting agencies play a vital role in the ability for Americans to obtain instant access to credit for large purchases, which is arguably a positive effect of their presence in the United States. The problems with the release of the information is the presence of errors. Byron Acohido and Jon Schwartz describe how "[a] prospective borrower filling out an online loan application can submit less than nine correct digits of Social Security number and just three matching letters of the first name of someone of good credit standing. Often that's enough to trigger the delivery of a credit report and subsequent

---

[932] *Ibid.*
[933] Finklea, K. M. (2010). *Identity Theft: Trends and Issues*. Congressional Reporting Service. Report to Congress.
[934] *Ibid.*
[935] *Ibid.*
[936] Hoofnagle (2009): 16.

approval for a new cell phone account or credit card..."[937] These three letters of the first name can be out of order or sequence and still trigger the delivery. The ease of delivery facilitates financial identity theft in part. For without the delivery of a credit report, financial service providers do not possess the credit rating of the applicant and this appears to decrease the odds of granting the applicant a new line of credit. It must be noted, however, how the consumer reporting agencies obviously face tremendous technical challenges to carry out their prime business of credit reporting.

The other mandate for consumer reporting agencies is more relevant to the prevention of financial identity theft. The placement of fraud alerts on the credit reports of consumers, usually previous victims of financial identity theft, is a responsibility of the agencies. These alerts ought to serve as a red flag for the financial service provider which requested the report.

Other similar, albeit arguably more effective, efforts include credit freezes. Such a freeze actually prevents access to the file of a consumer and as such also prevents the opening of a new line of credit. When a financial service provider attempts to gain access to the file, the consumer reporting agency must notify the consumer in an effort to unlock her file in order for it to be viewed by the financial service provider. In order for consumers to obtain a credit freeze they must contact all four consumer reporting agencies and send a letter accompanied by a fee. The fees generally range from $5 to $10.[938] Many states do not require a fee from victims of financial identity theft. Credit freezes are still a State led effort which began in California in 2003. As of December 29, 2009, forty-seven States had passed a credit freeze law.[939] The exceptions are Alabama, Michigan, and Missouri.[940] The discrepancy between State credit freeze laws leads to complications for residents of particular States. Kristan T. Cheng therefore calls for Federal credit freeze legislation which "…is available to all consumers and includes a quick thaw provision, specific creditor thaw, and reasonable fee structure [which] will provide consumers with superior and uniform identity theft protection."[941]

The potential for credit freezes to play a significant role in the prevention of financial identity theft is recognized by various sources. Hoofnagle discussed the idea of a credit freeze several years ago when he made the proposal to change the default state of credit reports from a 'liquid' to a 'frozen' state.[942] Such a change is necessary since "…our current credit system allows our personal information to flow like water to almost anyone who requests it. Once credit information is released, credit grantors who are operating in an extremely competitive market race to issue new tradelines. This makes it simple for impostors to commit identity theft by obtaining new credit accounts."[943] The proposed credit freeze system provides consumers with the power to 'thaw' the file when they desire to do so. And as such, consumers maintain the control of access with regard to the party,

---

[937] Acohido, B. & J. Schwartz (2008). *Zero-Day Threat: The Shocking Truth of How Banks and Credit Bureaus Help Cyber Crooks Steal Your Money and Identity*. New York: Union Square Press: 101.

[938] See http://www.consumersunion.org/campaigns/learn_more/003484indiv.html (last accessed July 13, 2010).

[939] *Ibid.*

[940] *Ibid.*

[941] Cheng, K. T. (2008). Identity Theft and the Case for a National Credit Report Freeze Law. *North Carolina Banking Institute*, Vol. 12: 271.

[942] Hoofnagle (2005): 3.

[943] *Ibid.*

place, and the context of access. The core promise of the credit freeze rests in the fact that "[c]reditors will not extend tradelines without a credit report, and thus under a frozen credit report system, impostors would have great difficulty in obtaining new accounts. The frozen system would also prevent businesses and others from obtaining credit reports without consumers' full consent, thereby limiting marketing and other impermissible uses of the report."[944] The credit freeze therefore manages to address various facilitating factors. These include the omission of receiving pre-approved credit card applications along with the prevention against other attempts at true name fraud. Unlike many other 'solutions' the idea of the credit freeze actually addresses part of the architectural vulnerability[945] of financial identity theft. The main challenge is the opt-in aspect of the system which requires consumers to take action.

Moreover, the credit freeze reduces the convenience of instant credit which generally goes against the benefits Americans, or those residing in the United States, derive from the system. The question, therefore, surfaces whether such a reduction in convenience is a worthy investment in light of the potential security the countermeasure can deliver.

5.3.2 The Netherlands

Since 1965, the Bureau for Credit Registration, or in Dutch *Bureau Krediet Registratie* (BKR), functions as the primary supervisory organ for credit reporting in the Netherlands.[946] According to its Statutes, the main objective of BKR is to advance the industry of financial services in a socially responsible manner, to minimize the risks for financial service providers, and to prevent exceeding on overdraft facilities for consumers.[947] Initially, the list of participants only included banks and financing institutions. Later on, others joined included municipal credit banks and saving banks. During the seventies, other parties also became participants. These included mail-order firms, mortgage banks, credit card organizations, and more recently retail traders who issue member credit cards. All in all, nearly every institution which engages in a form of consumer credit is part of the list of participants. This is the result of the legal mandate laid down in the Consumer Credit Act which states in Article 1 how those who extend credit lines must have a license to do so. Such a license also requires the holder to become a participant of the credit registration system, or basically to become a participant of BKR.[948] The Consumer Credit Act also requires license holders to conduct a credit check via BKR before extending a line of credit of more than 1000 euros.[949]

BKR is a non-profit organization and came about after a research committee concluded there was a need for positive registration of consumer credit.[950] Positive registration means BKR registers all forms of consumer credit rather than exclusively 'negative' consumer credit accounts. The main intent of positive registration is to prevent consumers from encountering potential problems. The

---

[944] *Ibid.*
[945] Solove (2003).
[946] Stichting Waakzaamheid Persoonsregistratie (SWP) (1988). Bureau Krediet-Registratie: Drie Miljoen Kredietnemers. *Privacy en Registratie* (2): 22 – 24.
[947] *Ibid.*
[948] Kabel, J. J. C. (2002). Centrale Kredietinformatie en verwerking van persoonsgegevens (I). *Privacy & Informatie*, Vol. 5 (6): 244 – 249.
[949] SWP (1988).
[950] *Ibid.*

credit registration system of BKR does not contain 'sensitive' information, according to the former director of the bureau, such as race, religion, employer, income, or the total financial deficit of a person.[951] The credit registration file of individuals present in the system contains their name, address, date of birth, and the relevant credit information of all participating organizations. This credit information includes the amount and the time frame of the contract, including the expiration or final payment date. When a delay in payment occurs, BKR uses a code to indicate this in the individual's file.[952] The credit registration system of BKR is maintained in a centralized and automated system.

Until the mid-eighties, BKR was a pretty 'passive' organization. According to Arie Rip, the director at the time, BKR simply registered whatever information the banks provided to them and released the requested information upon command of its participants.[953] The end of the eighties led to a change in the organization. BKR transformed itself into a more active organization. This was mainly the result of the introduction of the Dutch Data Protection Act which gave BKR more responsibility with respect to the correctness of the information maintained within its system. Even so, Jan Kabel notes how the duty listed in the Data Protection Act is focused on the effort made by the responsible party rather than an explicit obligation to verify all information received from the participants.[954] This change in responsibility, however, also led BKR to have a direct responsibility to the consumer.[955] To adhere to this responsibility, BKR developed a department within the organization to represent the interest of the consumer. The point of departure for BKR is that the consumer is allowed to know everything that is listed in her name. Former director Rip notes during an interview how BKR has always been 'privacy-minded.' This claim is supported by the fact that in 1973 BKR provided consumers the right to view their own file.[956] This must be done in person through a participant organization and costs 4.95 euros. BKR specifically acknowledges the potential risks associated with requests over the telephone and via the Internet. Especially since imposters may want to request the copy of a credit history of another person. As a result, individuals need to request a copy in person and demonstrate an appropriate form of government-issued identification. Participants, on the other hand, can request and obtain the information on-line.[957]

Besides the right to view their own file, consumers also maintain other rights. Consumers maintain the right to request a list of participants who have requested to see their file during the previous year.[958] As Rip notes, such information is particularly interesting for consumers since they can use such information to verify that the information is actually requested with the proper objective. This type of request or consumer right serves as a warning to financial service providers to make sure they use the credit check in a considerate manner. Rip does state how the number of requests for such an overview is limited and is usually carried out by individuals who suspect something.[959] When BKR discovers unacceptable

---

[951] *Ibid.*
[952] *Ibid.*
[953] Gerards, J. L. & E. J. Snijders (1993). De toekomst van Tiel: Bureau Registratie? *Bank-en Effectenbedrijf*, November 1993: 6 – 11.
[954] Kabel (2002): 247.
[955] Gerards & Snijders (1993).
[956] *Ibid.*
[957] Kabel (2002): 246.
[958] An overview costs 4.95 euros.
[959] Gerards & Snijders (1993).

behavior with respect to credit file requests by its participants, it can issue a warning, monetary fine, or even a suspension.[960]

When a financial service provider rejects a credit application, the provider must provide the reason for the rejection. This must be done in a way which allows the applicant to judge whether the decision is based on complete and correct information.[961] When disagreements between participants and credit applicants occur, and they are incapable of resolving the issue amongst themselves, they can turn to the independent BKR arbitration board. The decision provided by the arbitration board is binding and appealing is generally not an option.[962]

BKR is a member of the Association of Consumer Credit Information Suppliers (ACCIS) which is an international group where various European credit registration bureaus reunite. The idea to develop such an association originated after BKR received criticism from the European Commission because its rules and regulations stated how only institutions based in the Netherlands could become participants of BKR. In response to the criticism, BKR changed its rules and regulations but encountered numerous challenges. The most relevant challenge was how does BKR determine the legitimacy of organizations which do not reside in the Netherlands. Especially due to the sensitive nature of the information, the potential for providing illegitimate organizations with such information became a cause for concern. As a result, BKR decided to contact partner organizations and develop an association with other organizations to discuss the challenges and to determine possible responses.[963]

Perhaps the most striking feature of BKR, especially in comparison to its American counterparts, is its share in fraud prevention. Besides credit registration, BKR began to play a role in fraud prevention after the organization came to the conclusion it was in a good position to contribute to such prevention. Even in 1993, Rip emphasizes the need for good identification due to the continuous increase in fraud. He particularly mentions the escalating trend of falsification and the theft of identification documents.[964] Within that framework, BKR in cooperation with the investigation department payment traffic developed the VIS system, which stands for verification information system.[965] This system allows financial service providers to verify whether identification documents presented during the (credit) application process are stolen. This verification occurs based on the number present on the document. BKR proved to be the ideal distribution channel since the organization has an infrastructure which focuses its services on all financial service providers. The system was later expanded to include all stolen and previously lost identification documents.[966]

---

[960] *Ibid.*
[961] Kabel (2002): 245.
[962] Kabel, J. J. C. (2003). Centrale Kredietinformatie en verwerking van persoonsgegevens (II). *Privacy & Informatie*, Vol. 6 (1): 4 – 10.
[963] Gerards & Snijders (1993).
[964] *Ibid.*
[965] *Ibid.*
[966] *Ibid.*

5.4 Account Activity

The abuse of existing accounts remains an area of discussion from a conceptual standpoint. As the discussion in chapter 2 illustrated, many financial service providers reject the inclusion of account takeover as a type of financial identity theft. This rejection is predominantely motivated by the desire to exclude such incidents from statistical overviews. The argument set forth by the industry generally states how account takeover supposedly presents less negative consequences to the individual victims in comparison to other forms of financial identity theft, especially true name fraud. This is because victims of account takeover often manage to retrieve the lost funds. As Heather M. Howard notes 'true name fraud' "…takes a greater toll on its victims than does account theft: their financial losses are more substantial, more difficult to discover, and take considerably longer to resolve."[967] The importance of the incorporation of account takeover rests in its exposure of opportunities in the infrastructure of financial services. Moreover, whereas often existing clients receive a refund for the lost financial assets, there is still an inconvenient and time consuming process involved in response to the problem, especially when the victim lives paycheck to paycheck.

5.4.1 United States

Credit and payment card fraud are familiar characters and their presence dates back several decades. The section on unsolicited credit cards already provided a brief insight into the problems associated with credit cards, and this section depicts another dimension of the problem. From a physical perspective, credit and payment cards have encountered challenges due to the sensitivity of the black magnetic stripe on the back of the card to counterfeiting.[968] This is a well known vulnerability.

Other means of facilitation of financial identity theft came about through the introduction of Internet banking. The introduction of Internet banking in the United States occurred during the end of the previous century. According to the GAO, approximately 17 per cent of all banks, savings associations, and credit unions in the United States, offered some form of internet banking.[969] In total, 20 per cent of these depository institutions maintained fully transactional websites in 1999.[970] The ability to conduct transactions via the Internet introduced novel challenges. The GAO identifies how banking via the Internet heightens a variety of previously existing risks including security, transactional, strategic, reputational, and compliance risks.[971] For financial identity theft, the focus remains on security and transactional risks. Security risks, according to the GAO, include "...the risk of potential unauthorized access to a depository institution's networks, systems, and databases that could compromise internal systems and customer data and result in

---

[967] Howard, H. M. (2005). The Negligent Enablement of Imposter Fraud: A Common Sense Law Claim. *Duke Law Journal*, Vol. 54: 1266.
[968] Mandell, L. (1990). *The Credit Card Industry: A History*. Boston: Twayne Publishers.
[969] Government Accountability Office (GAO) (1999b). *Enhancing Federal Oversight of Internet Banking Activities*.
[970] The GAO defines fully transactional sites as sites which offer capabilities such as real-time account queries, transfers of funds among accounts, bill payments, or other banking services.
[971] GAO (1999b): 8-9.

financial losses."[972] The study of the GAO in 1999 proved relatively premature due to the youthful nature of Internet banking in the United States. Despite the narrow number of examinations of depository institutions and problems associated with their presence on the Internet, the GAO concludes how "...the examinations we reviewed revealed that some depository institutions had not taken all the necessary precautions to mitigate on-line banking risks."[973]

Whereas the GAO identifies how regulatory agencies provided guidance to depository institutions to mitigate the risks of Internet banking, the implementation of Internet banking originally occurred without formal interference from the Federal government. According to Anita K. Pennathur, "[t]he federal government's position was that it did want to impose regulation prematurely and thereby stifle a process that was still in its infancy."[974] Pennathur goes on to quote former Federal Reserve Chairman Alan Greenspan who proclaimed in 1996 how "[i]f we wish to foster financial innovation, we must be careful not to impose rules that inhibit it."[975] Advice from the five regulatory agencies[976] therefore proved to be the next best thing. These agencies offered additional guidance on August 8, 2001 through their publication of *Authentication in an Electronic Banking Environment*.[977] The primary focus of the guidance was "...on risk management controls necessary to authenticate the identity of retail and commercial customers accessing Internet-based financial services."[978] The guidance emphasized its neutrality toward all technologies and instead highlighted the importance of customer verification in an electronic banking environment. "An effective authentication system" according to the agencies, "...can help financial institutions reduce fraud and promote the legal enforceability of their electronic agreements and transactions. Strong customer authentication practices also are necessary to enforce anti-money laundering measures and help financial institutions detect and reduce identity theft."[979] Overall, the guidance merely provides a synopsis of the importance of customer authentication mechanisms. Through the guidance, the agencies attempt to encourage and persuade depository institutions to re-evaluate existing means of authentication, predominantly the single factor username-password, used by most banks in the United States.

Several years later, in 2004, the FDIC published a study on unauthorized access to financial service providers and described in its findings how financial service providers should consider a number of steps including upgrading from a single factor authentication system to a two factor authentication system.[980] The FDIC states in its study how "[t]wo-factor authentication is significantly more secure than single-factor authentication because the compromise of one factor would not be enough to permit a fraudster to access the system and the additional

---

[972] *Ibid:* 8.
[973] *Ibid:* 23.
[974] Pennathur, A. K. (2001). "Clicks and bricks": e-Risk Management for banks in the age of the Internet. *Journal of Banking & Finance*, Vol. 25: 2117.
[975] *Ibid.*
[976] These are the Federal Deposit Insurance Corporation (FDIC), Federal Reserve System (FRB), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and Office of Thrift Supervision (OTS).
[977] Federal Financial Institutions Examination Council (FFIEC) (2001). *Authentication in an Electronic Banking Environment.*
[978] *Ibid:* 1.
[979] *Ibid.*
[980] Federal Deposit Insurance Corporation (FDIC) (2004). *Putting an end to account-hijacking identity theft.*

factor (usually a token or biometric identifier) is extremely difficult to compromise."[981] Multiple factor authentication mechanisms combine at least two types of authentication. These types of authentication are generally divided into three categories:

1. Something the consumer *knows*
2. Something the consumer *has*
3. Something the consumer *is*

The majority of banks in the United States appear to rely on a single factor authentication composed of something the consumer *knows*. The FDIC acknowledges the vulnerability of such a system especially as a result of the proliferation of phishing attacks and the vast usage of malicious software which manages to capture the keystrokes entered onto the screen. As a result, the FDIC encourages the usage of an additional factor for the authentication of bank clients.

The following year, in 2005, the Federal Financial Institutions Examination Council (FFIEC) issued another guidance. The *Authentication in an Internet Banking Environment* guidance replaced the previously issued guidance. Its additional value remains difficult to assess. The FFIEC itself justifies the renewed guidance through writing "[s]ince 2001, there have been significant legal and technological changes with respect to the protection of customer information; increasing incidents of fraud, including identity theft; and the introduction of improved authentication technologies."[982] Certainly these reasons are both accurate and valid; yet, the approach remains the same. The FFIEC attempts to softly push the depository institutions in the appropriate direction and identifies the inadequacy of single factor authentication mechanisms. Simultaneously, the Agencies appear to contradict themselves when they write the following response to a question listed in a frequently asked questions document developed to assist banks in the implementation of the guidance. The question posed is whether the guidance *requires* the use of multiple factor authentication, to which the Agencies respond, "[n]o, the guidance does not call for the use of multifactor authentication."[983]

Guidance combined with self-regulation proved incomplete for the mitigation of risks for banking in an online environment. The idea of and the support for self-regulation came under pressure after it became evident how the lack of advanced means of security granted perpetrators of financial identity theft the opportunity to drain accounts of clients. Certainly, the single factor system offered convenience for the clients, but introduced vulnerabilities for them as well. The main fear on the side of the banking industry appears to be the potential loss of clients as a result of the 'complexity' involved in multiple factor authentication mechanisms. This fear is not unfounded. Jane M. Kolodinsky *et al.* demonstrate how simplicity is a significant positive factor for consumers to adopt internet banking.[984]

Accordingly, the focus on access to online services became convenience rather than security in the United States. Single-factor authentication of clients became

---

[981] *Ibid:* 26.
[982] FFIEC (2005). *Authentication in an Internet Banking Environment.*
[983] FFIEC (2006). Frequently Asked Questions on FFIEC Guidance on *Authentication in an Internet Banking Environment*.
[984] Kolodinsky, J. M., Hogarth, J. M. & M. A. Hilgert (2004). The adoption of electronic banking technologies by US consumers. *The International Journal of Bank Marketing,* Vol. 22 (4): 238-259.

the norm. As the FFIEC notes, single-factor authentication, as the only control mechanism, is "…inadequate for high-risk transactions involving access to customer information or the movement of funds or parties."[985] A growing body of literature clearly states the need for multi-factor authentication and claims that the majority of current authentication means used by banks within the digital environment are inadequate.[986] According to results published by Javelin Strategy & Research in 2007, multi-factor authentication (MFA) systems in online channels are active in 88% of banks.[987] This study, however, only takes into consideration the 25 top banks in the United States.

Even so, as shall become painfully apparent in section 5.4.2, multiple factor authentication systems also remain vulnerable and are, as such, not as difficult to compromise as the FDIC stated in its study. Several years ago, when the FFIEC published its second guidance for internet banking authentication systems, Bruce Schneier labeled two-factor authentication as 'too little, too late.'[988] Schneier proclaimed how "[t]wo-factor authentication isn't our savior. It won't defend against phishing. It's not going to prevent identity theft. It's not going to secure online accounts from fraudulent transactions. It solves the security problems we had 10 years ago, not the security problems we have today."[989]

Besides increased authentication mechanisms to prevent unauthorized account access and activity, the financial services industry also incorporates software intended to detect fraud based on patterns. These fraud detection mechanisms flag suspicious transactions. This can occur through the use of behavior models, where the development of a pattern arises through all transactions carried out by the account holder. When a transaction fails to fit the pattern, the mechanism flags the transaction as suspicious. The main problem with the use of behavior models as a means for fraud detection is the potential for a change in the behavior of the actual account holder, which means certain transactions are flagged as fraudulent while they are indeed legitimate.[990]

Another means of fraud detection looks at transactions in a more isolated manner through observing other aspects of the transaction. As C. Withrow *et al.* note, "[a] transaction might arouse suspicion if, for example, it is for a large amount of money and with a particular type of merchant (e.g. online bookmaker) at a certain time of day."[991] Whereas the behavior model uses a fraud detection strategy at the account level, the other strategy focuses more on the transaction level. Still, neither of these approaches is perfect, and understandably so. Vishal Vatsa *et al.* describe how the employment of rule-based schemes suffer from "...the limitation that in a repeated game environment, a fraudster can eventually learn the defense mechanism adopted by the FDS."[992]

---

[985] FFIEC (2005).

[986] See for example Clayton, R. (2005). Insecure real-world authentication protocols (or why phishing is so profitable). *Proceedings of 13th International Workshop on Security Protocols.*

[987] Javelin Strategy & Research (2007b). New Report Shows Top U.S. Banks Succeeding in Identity Fraud Resolution, Slower Progress In Detection and Prevention Capabilities. *Press Release.*

[988] Schneier, B. (2005). Two-Factor Authentication: Too Little, Too Late. *Communications of the ACM*, Vol. 48 (4): 136.

[989] *Ibid.*

[990] Withrow, C., Hand, D. J., Juszczak, P., Weston, D. & N. M. Adams (2009). Transaction Aggregation as a Strategy for credit card fraud detection. *Data Mining and Knowledge Discovery*, Vol. 18 (1): 30 – 55.

[991] *Ibid:* 31

[992] Vatsa, V., Sural, S. & A. K. Majumdar (2005). A Game-theoretic Approach to Credit Card Fraud Detection. *Proceedings of the International Conference on Information Systems Security*, Lecture Notes in Computer Science, Vol. 3803: 263 – 276.

5.4.2 The Netherlands

The introduction of transferable money ('giraal geld') ended the hegemony of cash in the Netherlands. Compared to other countries, the Netherlands joined the advances in methods of payment relatively late. The main invention became the *pinpas*, or the debit card, which was introduced in the Netherlands in 1982.[993] The Gemeentegiro Amsterdam issued *giropassen* in 1961 which contained the same function and look as the later more broadly distributed *pinpassen*. In the media, the introduction of the *pinpas* proved to be a welcomed alternative since consumers simply needed to carry the card and retailers received their money faster than through the use of credit cards.[994] During the mid-eighties the card obtained a life of its own. Whereas its original function was to serve as a means of identification when cashing a check, due to the black magnetic stripe on the back of the card and the usage of a pin number its functionality grew. First, banks introduced automatic teller machines for clients to obtain cash. The second application became the ability to use the plastic cards in stores to purchase goods. The *pinpas* maintained an attractive character due to its accessibility. Unlike with credit cards, clients did not need to meet an income threshold in order to receive and be able to use the card.

Despite the many advantages, the *pinpas* also came accompanied with various concerns and vulnerabilities. In particular uncomfortability and insecurity along with worries about the level of fraud resistance implemented in the card dominated the debate of disadvantages.[995] Newspaper articles during the late eighties expressed considerable concern about the vulnerability to fraud inherent in the *pinpas* system. The Association of Consumer Affairs led the movement. Nevertheless, banks and other relevant financial service providers, convinced of the benefits, continued to expand the system and issue the cards.[996]

During the start of the twenty-first century various incidents rekindled the debate about the dangers associated with the more recent methods of payment. Most of the reported incidents centered around the duplication of the data from the black magnetic stripe on the back of the *pinpas* (also known as skimming) at various locations including, restaurants, gas stations, ATMs. Furthermore, perpetrators also managed to use stolen cards and disrupt the delivery of cards to their rightful owners. In its yearly overview of 2002, the Dutch Central Bank briefly refers to fraud with *pinpassen*, but also mentions how the number of incidents in relation to the overall number of transactions seems to be marginal.[997] Even so, banks introduced additional security measures, as a result of recommendations set forth by the Dutch Central Bank after having conducted a risk assessment due to the various fraud related incidents involving the *pinpas*.

Despite the brief remark issued by the Dutch Central Bank, other sources indicate how 2002 became the year citizens and banks in the Netherlands first began to encounter serious problems with respect to skimming.[998] During 2003

---

[993] Mooij, J. & T. Dongelmans (2004). *Mogen wij even afrekenen? Twee eeuwen betalen in Nederland.* Amsterdam: Boom.
[994] *Ibid:* 83.
[995] *Ibid.*
[996] *Ibid.*
[997] De Nederlandsche Bank (2003). *Jaarverslag 2002.*
[998] Korps Landelijke Politiediensten (KLPD) (2008). *Georganiseerde bovenregionale vermogenscriminaliteit Verslag van een onderzoek voor het Nationaal dreigingsbeeld 2008*.

and 2004, banks armed their ATMs with anti-skimming devices such as a plastic mouthpiece.[999] This measurement assisted the achievement of a decrease in skimming cases in 2005. Even so, the following year skimming returned when Equens, the primary payment processor, received incident complaints.[1000] In 2008, the Dutch Central Bank yet again identified the increase of skimming cases during the previous year.[1001] The financial damage caused through skimming incidents demonstrated an escalating line during the period from 2005 (1.8 million euros) until 2007 (12.1 million euros).[1002]

In response to the increase, the Dutch Central Bank referred to its anticipation of the introduction of EMV technology. EMV technology, which stands for Europay Mastercard Visa, eliminates the usage of the black magnetic stripe and instead uses an EMV chip. This measure attacks the vulnerability displayed by the black magnetic stripe which proved particularly vulnerable for fraud through the ability of perpetrators to copy the information stored on the black stripe, which they subsequently managed to place on a blank card.

While the Dutch Central Bank mentions the introduction of EMV technology in response to the 2007 increase, the damage continued to escalate. The following year, in 2008, the Dutch Central Bank once again identifies an increase in skimming incidents, and even speaks of a 'considerable' increase in the number of cases.[1003] This appears to be because the deadline for the issuance of cards equipped with an EMV chip is set for the end of 2010.[1004] And, more importantly, the compliance data for all ATMs is 2011.[1005] Moreover, the Dutch Central Bank states how the entire payment traffic system shall use EMV technology in 2013 at the latest. As a result, the extensive period of transition provides perpetrators of financial identity theft with sufficient time to continue their operations.

The financial loss over 2009 was 36 million euro. This was an increase of 5 million in comparison to the previous year. Due to the publication of financial losses as a result of skimming, the phenomenon generally dominates the debate concerning fraud within the financial services industry. The vulnerabilities are physical since perpetrators of account takeover manage to make adjustments to the ATM which allow them to obtain the data on the black magnet stripe and also capture the pin code needed to drain the accounts.

Simultaneously, problems with Internet banking are also on the rise. This is difficult to detect due to the lack of available information on the actual damages suffered as a result of unauthorized access via the Internet to bank accounts. In 2008, the Dutch Central Bank identified an increase in fraud with regard to internet banking, but fails to mention actual figures.[1006] These did not come about until October 2010, when the Dutch Banking Association finally revealed an inside peek into the number of incidents and the financial damage caused by Internet banking related fraud. The media story about the data release speaks of a significant rise in the number of Internet banking related fraud incidents.[1007] This

---

[999] *Ibid.*
[1000] *Ibid.*
[1001] De Nederlandsche Bank (2008). *Jaarverslag 2007*.
[1002] KLPD (2008).
[1003] De Nederlandsche Bank (2009a). *Jaarverslag 2008*.
[1004] De Nederlandsche Bank (2009b) *SEPA Migration Plan for the Netherlands*. Status and Planning June 2009.
[1005] *Ibid.*
[1006] De Nederlandsche Bank (2008).
[1007] 'Fraude internetbankieren fors gestegen' (2010). Available at:

headline is the result of a comparison between the number of incidents in 2009, which was 154, and the number of incidents during the first half of 2010, which was 541. The financial damage also experienced an increase. The financial loss in 2009 was 1.9 million euros as opposed to 4.3 million euros during the first half of 2010. The Dutch Banking Association also took advantage of the release of the data to introduce yet another public awareness campaign as a means to reduce the crime.

Problems with Internet banking in the Netherlands came as a bit of a surprise since the system actually departed from an emphasis on security rather than convenience. Unlike the United States, the Netherlands introduced multiple factor authentication mechanisms from the start. Whereas the United States contains many financial service providers which use single factor authentication mechanisms, most often something the consumer *knows* (i.e. username and password), banks in the Netherlands use a combination of something the consumer *knows* and something the consumer *has*. When several banks desired to use the Internet as a channel for communication and transactions with their clients, the Dutch Central Bank immediately expressed its concern about the security of such a system and required the banks to implement a mechanism which surpassed the mere usage of a username and password.[1008] Therefore, the major Dutch banks introduced a two-factor authentication system from the start in anticipation of the vulnerability associated with a single factor authentication system. Wim Hafkamp and René Steenvoorden emphasize this decision when they write, "[f]rom the early beginning of Internet direct banking in the Netherlands which started somewhere around 1997, security played an important role in the architectural design. Authentication of the customer and the integrity of the transaction are and were key starting points."[1009] Several banks, including the ING Bank, ABN Amro, Fortis and the Rabobank all began to use randomizers combined with a password. These randomizers are small tokens which look like simple calculators. Randomizers generate random numbers for consumers to enter when they try to log on to their account online. In order for consumers to log on to their accounts they must insert a username onto the screen. Furthermore, consumers must enter their passcode into the randomizer and then enter the number which appears on the screen into the randomizer. Subsequently, the randomizer generates a number which they must then enter onto the screen before they can access their account information.

A variation of this system uses TAN-codes rather than randomizers. The Postbank, which is now part of ING bank, uses this system. Certain other banks also require consumers to insert their debit card into the randomizer before the device is activated. In May 2010, the ING bank removed the need for the randomizer for Internet banking and shifted over to the usage of username and password for entry into the system. To carry out transactions, on the other hand, consumers receive tan-codes via text messages to their mobile phones. When consumers are not in a possession of a mobile phone, they receive the TAN-codes via regular mail.

---

http://www.nrc.nl/economie/article2631471.ece/Fraude_internetbankieren_fors_gestegen (last accessed on October 16, 2010).

[1008] Interview *De Nederlandsche Bank*, January 12, 2010, Amsterdam.

[1009] Hafkamp, W. & R. Steenvoorden (2009). 'Experience From the Financial Sector with Consumer Data and ICT Security,' in Z. Lukszo, G. Deconinck & M. P. C. Weijnen (eds.) *Securing Electricity Supply in the Cyber Age*, Springer Netherlands: 159 – 169.

The security of two-factor authentication mechanisms has been prone to skepticism once incidents began to arise. After incidents of identity theft surfaced about the use of online banking in Belgium in October 2007, the Dutch Association for Banking stated how, "[o]nline banking in the Netherlands is safe."[1010] Cases of identity theft through misuse of online banking services only happen incidentally. A representative of the Association also states how the Dutch online banking system seems to be one of the most secure systems in the world. Both the Association and the Dutch Consumer Union claim how many times incidents of identity theft occur after successful social engineering attacks which manage to fool the consumer, which means the banks do not play a facilitating role in the incident.[1011]

The occurrence of man-in-the-browser (MITB) attacks exposed the vulnerabilities of Internet banking in the Netherlands. As Hafkamp and Steenvoorden note, "[d]espite the use of strong authentication banks in the Netherlands were faced with serious, sophisticated malware-attacks against their Internet direct banking applications since the beginning of 2007."[1012] Despite the level of security offered by banks in the Netherlands, sophisticated perpetrators of financial identity theft still managed to drain bank accounts of clients. The MITB attack circumvents the two-factor authentication means through placing the perpetrator between the client and the bank. This occurs through the use of Trojan horses. Whereas perpetrators of traditional phishing attacks develop fraudulent websites to obtain the credentials of clients, victims of MITB attacks actually arrive at the legitimate website of their financial service provider. Yet, through interjecting themselves between the client and the bank, perpetrators manage to receive the communication from both sides. The threat of MITB attacks is strengthened through the ability of perpetrators to manipulate both the communication as well as the presentation layer. The feedback option used by banks therefore becomes irrelevant since perpetrators also manage to manipulate the information provided to the clients. This means clients cannot detect the fraudulent transactions through the feedback they receive from the 'bank.'

The success of MITB became evident when 200 clients of the ABN Amro bank downloaded an executable file which installed a Trojan horse on their computers which subsequently compromised the browser to become the man-in-the-middle. Perpetrators managed to drain the accounts of the clients (see section 3.2.2).

To respond to the enhanced threat against the Internet banking system in the Netherlands, banks have responded in both an individual and a collaborative way. Hafkamp and Steenvoorden categorize these responses into four categories including secure the channel, educate the consumer, clean the Internet, and monitor transactions. In order to secure the channel, banks have tried to introduce variations on the existing authentication mechanisms. This occurs through changes in the dialogue. This can come about through additional means of verification such as the use of text message via mobile phones or adding challenge-response options to the randomizer which asks clients to verify the

---

[1010] 'Internetbankieren is veilig in Nederland' (2007). Available at: http://www.nu.nl/news/1265153/50/rss/%27Internetbankieren_in_Nederland_is_veilig%27.html (last accessed on July 5, 2010).
[1011] *Ibid.*
[1012] Hafkamp & Steenvoorden (2009): 165.

amount entered or the account number of the recipient of the transaction.[1013] As noted above, the ING bank decided to change its system and introduce a single factor authentication for the login process, which means clients who simply want to look at their bank account details no longer need an additional means of authentication. In order to carry out transactions, on the other hand, the bank sends TAN codes via text messages or regular mail, which is a different 'channel.'

The second type of response to the increased threat is consumer education which is largely the result of a cooperative effort between banks and the Dutch Banking Association in the Netherlands. This cooperative effort resulted in the consumer awareness campaign *3x kloppen* which means knocking three times and explains to clients how to check three aspects including the security of their computer, the URL of the bank, and the entered payments. The effectiveness of this response seems limited due to the inability of consumers to observe the presence of Trojan horses and as such the occurrence of MITB attacks.

The third response is to clean the Internet. This response category includes actions such as the attempt to eliminate drop zones. Drop zones are criminal owned servers which collect information from infected computers. In the same category, Hafkamp and Steenvoorden also note how "[i]n the beginning of 2009 Banks in the Netherlands jointly developed a service to detect malware threats on the Internet and to respond quickly in the event that a bank is hit by malware."[1014] The last type of countermeasure is transaction monitoring which receives substantial attention, especially since the industry believes how such analyses can expose unusual patterns in an effort to prevent identity theft before its occurrence (see section 5.4.1).[1015]

The evolution of other applications also deserves a brief moment of reflection. The Rabobank in the Netherlands offers the option to make payments via mobile phones.[1016] To participate in the mobile banking application of the Rabobank, participants need a mobile phone which supports a secure internet connection. The mobile phone application provides for electronic transfers with a maximum of 300 euros and a maximum of a 1000 euros per week. Payments above 300 euros in a single transaction can only be completed through the usage of the random reader. The combined use of the mobile phone and the random readers allows for an electronic transfer with a maximum of 50,000 euros. The mobile payments system only allows electronic transfers to accounts which have been engaged in transfers during the last fifteen months. If a participant desires to make an electronic transfer to an unknown account, the participant must engage the random reader for its completion. The mobile banking application also allows participants to check their account balance.[1017]

Just as the Rabobank allows its clients to engage in mobile banking, the bank also provides an application for mobile payments. This application allows participants to make payments through the use of the mobile phone number of the other person. This service is not restricted to Rabobank clients and is available to anyone in the Netherlands with a mobile phone and a bank account. Basically,

---

[1013] *Ibid.*
[1014] *Ibid*: 167.
[1015] *Ibid.*
[1016] See for general information: http://www.rabobank.nl/particulieren/producten/modern_bankieren/via_mobiele_telefoon/rabo_mobielbankieren.html
[1017] The first 52 times within one year are free.

mobile payments allow participants to install a mobile wallet. The participant then deposits money into the wallet and can make payments or purchase goods through sending text messages.[1018]

5.5 Conclusion

As indicated in the introduction financial service providers generally play a vital role in the facilitation of financial identity theft. This is primarily evident through the facilitation of the second stage of the crime by financial service providers. Such facilitation can occur during different moments of interaction between the perpetrator and the financial service provider. During the acquisition process, perpetrator may take advantage of marketing instruments which endanger consumers due to the emphasis on convenience rather than security. This became evident through the background analysis of the credit card industry in the United States. The description of the United States demonstrated the crucial transition of the credit card from an instrument of the upper-middle class down to a tool for the masses. This transition required the industry to engage in serious competition over prospective clients. Such competition occurred through the introduction of aggressive marketing techniques involving low-threshold application methods, if any, which exposed consumers to vulnerabilities of financial identity theft. The apparent focus on competition and financial profit overshadowed the security concerns associated with these practices. Whereas officials from the industry proved aware of the complications, they prioritized the acquisition of clients and the potential for maximization of profits.

In contrast to the United States and its relationship with credit cards, the Netherlands demonstrates an entirely different story. In a country where the banking industry provides sufficient alternatives in the area of methods of payment, Dutch consumers never appeared to be attracted to the idea of credit which meant the credit card failed to obtain a similar level of popularity. This is an important distinction between the United States and the Netherlands since the exposure of potential dangers due to aggressive marketing techniques introduced by the credit card industry remained absent in the Netherlands.

Besides the acquisition process, the application process also proved a vital business practice with regard to the potential facilitation of financial identity theft. For credit cards, the application process, where the credit card companies must verify the identity of the prospective clients, has been reduced to a mere formality. The importance of the application process for banks extends beyond the potential for financial identity theft and also concerns other potential abuses of the financial sector. Prime examples include tax evasion, money laundering and terrorist financing which have all played a role in the development of the legislation which governs the manner through which banks conduct their application processes.

The role of consumer reporting agencies in the application process also became apparent. The release of a credit report occurs with relative ease in the United States which facilitates financial identity theft since financial service providers generally consider such a report an essential aspect of the verification process. The historical evolution of consumer reporting agencies demonstrates the

---

[1018] See generally:
http://www.rabobank.nl/particulieren/producten/modern_bankieren/via_mobiele_telefoon/rabo_sms_betalen

near neglect for consumers and their rights. This is in contrast to the treatment of consumers by the Dutch credit registration bureau which grants consumers rights without the need for governmental interference. Moreover, BKR recognized its integral position in the credit granting process and voluntarily became part of a fraud prevention tool development.

On the account activity front, both the United States and the Netherlands encountered challenges as a result of the vulnerability to fraud of the black magnetic stripe. This vulnerability occupies a dominant place in the debate on account takeover in the Netherlands, especially as financial damage continues to escalate. Besides the physical vulnerabilities, Internet banking activities also increased the presence of suitable targets for account takeover. The banks in the United States demonstrated an emphasis on convenience through the implementation of single-factor authentication. The Netherlands instead provided for a more balanced approach between security and convenience through the introduction of a two-factor authentication system. Nevertheless, the arrival of MITB attacks exposed vulnerabilities which prove difficult to mitigate. Unlike traditional phishing attacks, clients are less likely, if at all, to detect the man in the browser. Bruce Schneier anticipated the vulnerabilities associated with the two-factor authentication mechanisms in 2005 when he wrote, "[e]arly adopters of this technology may very well experience a significant drop in fraud for a while as attackers move to easier targets, but in the end there will be a negligible drop in the amount of fraud and identity theft."[1019] As a result, the continuous advancements made by perpetrators with respect to their methods have engaged the financial industry into a rat race which challenges banks to maintain an acceptable balance between security and user convenience. The best state of affairs then to achieve appears to be reasonable insecurity.[1020]

[1019] Schneier (2005).
[1020] Etalle, S. (2008). *Nice to Know*. Inaugural lecture. Eindhoven University of Technology, October 3, 2008.

6 | Consumers

On July 27, 2009, the Ministry of Justice of the Netherlands launched a large public awareness campaign to prevent citizens from falling victim to cybercrime.[1021] During five weeks, the campaign which features a fictional character 'Sandra', was seen on television and heard on the radio. In the commercial used for the campaign, Sandra reveals all. Her bank account number, pin code, log-in name, and video tapes of her holiday at the beach are made public. Sandra herself watches and listens as people gather on the street to witness the publication of all her information. She appears flabbergasted. She is the perfect depiction of the unaware and naïve citizen. Security on the Internet, the campaign claims, is in *your* hands.[1022] To consider consumers, or citizens, as facilitators of financial identity theft is controversial, especially since such considerations maintain the potential to enter a slippery slope into the realm of blaming the victim. As a result, this chapter features a different approach from the previous three due to its more normative character as a means to make a contribution to the ongoing discussion on consumers as facilitators of financial identity theft. The ongoing discussion focuses primarily on the degree to which consumers maintain both the ability and responsibility to 'prevent' or at least reduce the risk of financial identity theft. Fred H. Cate describes how the most basic privacy protection is personal judgment and how the vital role of consumers in privacy protection is mostly ignored in discussions about the topic.[1023] Cate uses this notion to expand his argument and claims how the actions of individuals may provide the best defense against identity theft. "Despite all of the bills that have been introduced to combat identity theft, many of the most effective means continue to be those that individuals take to protect themselves: keeping a close watch on account activity; reporting suspicious or unfamiliar transactions promptly; properly destroying commercial solicitations; storing valuable documents securely; protecting account names and passwords; and never disclosing personal information to unknown callers."[1024] The research results provided by Javelin Strategy & Research (see section 1.1.2) are in turn used as a means to substantiate this argument.

The advice offered to consumers and the argument set forth about the ability of consumers to reduce the risk of financial identity theft receives resistance. Daniel Solove rejects the general advice provided by Cate and others about the correlation between individual action and identity theft risk reduction. In particular, Solove states how even if individuals did take all steps advised to them, significant risk reduction still fails to occur.[1025] This lack of significant risk reduction is due to the actions of both the public and the private sector, which play a more prominent role in the facilitation of financial identity theft, accordinG

[1021] See http://www.nederlandveilig.nl/veiliginternetten/

[1022] In Dutch the slogan is: "veilig internetten heb je zelf in de hand."

[1023] Cate, F. H. (2001). The Privacy Paradox. *76th Annual Winter Newspaper Institute North Carolina Press Association*.

[1024] *Ibid:* 9.

[1025] Solove, D. J. (2003). Identity Theft and the Architecture of Vulnerability. *Hastings Law Journal*, Vol. 54: 1227 – 1273.

to Solove. Others support this notion.[1026] In the overall problem, consumers are victims rather than facilitators. Their share in the enablement of the problem is minimal, if existent at all. Certain sources even consider the emphasis on individual responsibility a mere political strategy to divert the attention away from the 'actual' facilitators.[1027] A similar sentiment is echoed by Marron when she states: "[t]he problem becomes pitched not as one of systemic institutional culpability, but as lack of awareness on the part of individuals."[1028] According to Deborah Stone stories of 'inadvertent cause' are common in social policy.[1029] Individuals 'cause' many problems such as poverty, malnutrition, and disease, because they fail to understand the harmful effects of their willful actions. "Inadvertence here is ignorance;" Stone writes, and "the consequences are predictable by experts but unappreciated by those taking the actions. These stories are soft (liberal) versions of blaming the victim: if the person with the problem only changed his or her behavior, the problem would not exist."[1030] This chapter aims to provide a more comprehensive perspective on the potential facilitation of financial identity theft by consumers in an effort to add another dimension to the existing discussion on consumer ability and responsibility. The chapter commences with a brief overview of consumers as victims, which is based on limited research conducted to evaluate the correlation between demographics and the likelihood of victimization. Subsequently, through a categorization of types of consumer facilitation, this chapter aims to differentiate and demonstrate how the evolution of the methods used by perpetrators has led to a crucial expansion of ways to take advantage of consumers, and how the consumer's ability to actively control the facilitation process is slowly, but surely, diminishing. Since this is a general, or rather 'global' trend, no distinction is made between the United States and the Netherlands in contrast to the previous chapters.

6.1 Consumers as Victims

To develop a better understanding about the likelihood of consumers falling victim to financial identity theft, previous research aimed to unravel patterns with respect to the demographics of victims. These patterns do not imply nor provide any information on facilitating factors in themselves, but they do provide, or at least could provide, information on what makes certain consumers more vulnerable to financial identity theft. Research to explore which demographic characteristics make someone more likely to become a victim of financial identity theft is comparable to research conducted to unravel which individuals are more likely to get cancer or another potentially fatal disease. These risk factors, as a result, are not facilitating factors in the traditional sense as discussed throughout the chapter. Yet, they do play a role in financial identity theft and as such deserve attention. These factors are particularly interesting and relevant for all parties,

---

[1026] See for example Hoofnagle, C. J. (2005). 'Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors,' in A. Chander, L. Gelman, M. J. Radin (eds.) *Securing Privacy in the Internet Age*. Stanford, CA: Stanford University Press.
[1027] Whitson, J. R. & K. D. Haggerty (2008). Identity theft and the care of the virtual self. *Economy and Society*, Vol. 37 (4): 572 – 594.
[1028] Marron, D. (2008). "Alter Reality" Governing the Risk of Identity Theft. *British Journal of Crime and Criminology*, Vol. 48 (1): 29.
[1029] Stone, D. A. (1989). Causal Stories and the Formation of Policy Agendas. *Political Science Quarterly*, Vol. 104 (2).
[1030] *Ibid:* 286.

rather than consumers alone. To return to the comparison with fatal diseases, doctors are more likely to pay attention to patients with particular characteristics which could increase the risk of, for example, cancer. As such governments and businesses, including financial service providers, could target the relevant consumers and perhaps provide them with more specialized assistance. David Adam Friedman, for example, describes various approaches to consumer protection one of which is defining a protected consumer group which "...is significantly different. Instead of racing to beat the next big scam and attempting to solve the fraud problem for the entire population, it carves out a category of consumers and provides that group with heightened protection. Policymakers may select a group according to any of three criteria: unique vulnerability, reticence to report victimization, or susceptibility to specific schemes."[1031] Friedman foresees a lot of potential in selecting one group for 'hyper-protection.'

Information on the demographics of victims is limited. Keith B. Anderson conducted a study to analyze whether certain citizens are indeed more likely to become victims of identity theft.[1032] For his study, Anderson used the information contained in the Consumer Sentinel database maintained by the Federal Trade Commission (FTC). This contains data on consumer victims who filed a complaint with the FTC. While Anderson initially acknowledges how "[o]ne does not do something to become a victim – it just happens to you"[1033], he also describes how "…a little deeper reflection suggests that this is really not the case. The risks faced by consumers do differ, and these differences may manifest themselves in differences across groups with different demographic characteristics."[1034] Without trying to blame the victim, Anderson identifies a number of factors which may increase the likelihood of identity theft victimization for certain consumers. He predicts that factors such as having a good credit record, engaging in more transactions, and having a higher income level may make a consumer more likely to fall victim to identity theft. Furthermore, Anderson also identifies the potential correlation between falling victim to identity theft and the place where a consumer does business and the victim's household composition. Anderson concludes in his study that "[t]he likelihood that a person will be a victim of identity theft does appear to be related to demographics."[1035] He identifies the following relevant demographic characteristics in particular: level of income, education, gender, age and household composition. The results furthermore indicate how the elderly run a lower risk to become victims of identity theft, but that households with only one adult are more likely to be victimized.

Other authors focus on specific groups in connection to identity theft to differentiate between vulnerabilities[1036], whereas Gina W. Lane aimed to unravel

---

[1031] Friedman, D. A. (2007). Reinventing Consumer Protection. *DePaul Law Review*, Vol. 57: 303.

[1032] Anderson, K. B. (2005). *Identity Theft: Does the Risk Vary With Demographics?* Federal Trade Commission, Bureau of Economics Working Paper No. 279.

[1033] *Ibid:* 11.

[1034] *Ibid.*

[1035] *Ibid:* 23.

[1036] See Sylvester, E. L. (2004). Identity Theft: Are the Elderly Targeted? *Connecticut Public Interest Law Journal*, Vol. 3 (2): 313 - 341; Carlson, E. L. (2006). Phishing for Elderly Victims: As the Elderly Migrate to the Internet Fraudulent Schemes Targeting Them Follow. *Elder Law Journal*, Vol. 14: 423 - 427; Johnson, I. D. (2010). Preventing Identity Theft and Other Financial Abuses Perpetrated Against Vulnerable Members of Society: Keeping the Horse in the Barn Rather than Litigating over the Cause and/or Consequences of His Leaving. *Pace Law Faculty Publications*.

demographic and geographical patterns of identity theft. Her results confirm previous results which demonstrate higher incidence rates of identity theft in Southwestern states and lower incidence rates in New England and the Northern Plains States.[1037] Moreover, Lane writes how "…identity theft appears to maintain the well-documented regional patterns of traditional larceny and theft crimes, thus indicating that geographically independent digital opportunities do not appear to eradicate the importance of place in criminal patterns."[1038]

6.2 Consumer Facilitation

6.2.1 'Voluntary' Facilitation

The term 'voluntary' is problematic because its usage within the current context can lead to misguided interpretations. Voluntary facilitation here mainly refers to information dispersion which is unprompted by the perpetrator. The term is mainly used to indicate the distinction between the current and the subsequent categories of facilitation, and does not carry any normative implications. The voluntary exposure of consumers' personal information can facilitate the first stage of financial identity theft. Perpetrators have developed methods to take advantage of such exposure. Among the most infamous methods is dumpster diving. Basically, unsuspecting consumers toss out various documents containing sensitive personal information. Perpetrators become aware of this and start rummaging through garbage cans in search of these documents. Many times, one document does not contain all of the necessary information, but perpetrators combine different pieces of garbage to complete the picture. Several years ago, receipts still contained valuable information including the full credit card and account number, which proved to be an attractive source for perpetrators. Overall, consumers would unwittingly and voluntarily present perpetrators with their valuable personal information. Dumpster diving, as a method, took advantage of the voluntary and active participation of consumers. Certain sources reemphasize the importance of this type of facilitation due to a marketing interest. Or, as indicated in chapter 1, an interest held by the sponsors of select survey research.[1039]

More recently, perpetrators have managed to take advantage in similar ways from consumers who dispose of old computers, which contain, yet again, valuable personal information. Even if consumers believe they have cleared their hard drive of all data, they are often wrong. The data erased on their hard drive can easily be recovered by perpetrators. Various authors acknowledge this vulnerability.[1040]

There are, however, other ways consumers 'expose' their personal information. Social networking sites such as Facebook and MySpace provide the ideal outlet to let everyone know nearly everything about oneself. Perpetrators could exploit the

---

[1037] Lane, G. W. (2008). *Geographies of Identity Theft in the U.S.: Understanding Spatial and Demographic Patterns, 2002-2006*. Master of Science Thesis Texas A&M University.

[1038] *Ibid:* 56-57.

[1039] Hoofnagle, C. J. (2007). Identity Theft: Making the Known Unknowns Known. *Harvard Journal of Law and Technology*, Vol. 21 (1): 98 – 122.

[1040] See for example Bennison, P. F. & J. P. Lasher (2004). Data Security Issues Relating to End of Life Equipment. *Proceedings of the 2004 IEEE International Symposium on Electronics and the Environment*; Valli, C. (2004). Throwing out the enterprise with the hard disk. *2nd Australian Computer, Networks & Information Forensics Conference,* School of Computer and Information Science, Edith Cowan University, Perth, Western Australia: 124-129.

availability of information through these outlets. Howard Rush *et al.* describe how due to their popularity social networking sites have become appealing places for perpetrators of cybercrime.[1041] This is due to a number of reasons. In addition to the vast amounts of personal information available on social networking sites, they also offer perpetrators of cybercrime the ability to use the sites to spread malware, spam, and scams on a massive scale. Furthermore, social networking sites are turning into an attractive marketplace for recruitment.[1042] With respect to social networking sites, academic researchers have expressed interest in user concerns, or rather a lack thereof, with regard to privacy and trust. As Ralph Gross & Alessandro Acquisti have concluded "[i]n our study of more than 4,000 CMU users of the Facebook…we have shown how unconcerned its users appear to privacy risks: while personal data is generously provided, limiting privacy preferences are hardly used; only a small number of members change the default privacy preferences, which are set to maximize the visibility of users profiles."[1043] Others also recognize how despite measures of self-censorship, the majority of users still share a large amount of personal information on Facebook.[1044] This willingness to share personal information surpasses the area of social networking sites. Through an experiment, Jens Grossklags & Acquisti demonstrate how "...most subjects happily accepted to sell their personal information even for just 25 cents, and virtually all subjects waived the option to shield their information."[1045] These various pieces of academic research along with the general perception of both the public and the private sector develop an image of the 'careless' consumer.

Leyla Bilge *et al.* furthermore add significant insights to the potential facilitation of financial identity theft through users of social networking sites.[1046] Through the presentation of an experiment which includes automated social engineering attacks, Bilge *et al.* demonstrate how perpetrators of financial identity theft can access personal information maintained on profiles of users. This occurs through, for example, profile cloning where perpetrators 'clone' the profiles of authentic users and request to be added as a friend. Perpetrators send these requests to the social network of the 'cloned' individual rather than to random strangers. From the experiment of profile cloning, Bilge *et al.* conclude how "...the friendship acceptance rate for the forged profiles was over 60% for all the forged accounts (in one case, being as high as 90%). The acceptance rate from unknown users was constantly below 30%...These results confirm that by forging profiles, an attacker can achieve a higher degree of success in establishing contacts with honest users than when using fictitious accounts."[1047] Based on the results of their

---

[1041] Rush, H. Smith, C., Kraemer-Mbula, E. & P.Tang (2009). *Crime online: Cybercrime and illegal innovation*. Research report NESTA.

[1042] *Ibid.*

[1043] Gross, R. & A. Acquisti (2005). Information Revelation and Privacy in Online Social Networks. (The Facebook Case). *Pre-proceedings version ACM Workshop on Privacy in the Electronic Society (WPES)*: 10.

[1044] Jones, H. & J. H. Soltren (2005). Facebook: Threats to Privacy. Unpublished manuscript. Available at: http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf (last accessed July 13, 2010).

[1045] Grossklags, J. & A. Acquisti (2007). When 25 cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information. *Workshop on the Economics of Information Security (WEIS)*: 14

[1046] Bilge, L., Strufe, T. Balzarotti, D. & E. Kirda (2009). All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks. Paper presented at the *18th International World Wide Web Conference*.

[1047] *Ibid:* 557.

experimental research, Bilge *et al.* provide suggestions for improvements of security on social networking sites. In their suggestions, the authors acknowledge how users continue to be the weakest link but improved security requires the involvement of the social networking sites. Bilge *et al.* provide the recommendation for social networking sites to provide more information on the authenticity of the friend request and the user who initiated the request.[1048]

Whereas Bilge *et al.* direct suggestions toward the sites as opposed to the users, James Grimmelman focuses on the users.[1049] Grimmelman states how "[i]t's temptingly easy to pin the blame for these problems entirely on Facebook. Easy—but wrong. Facebook isn't a privacy carjacker, forcing its victims into compromising situations. It's a carmaker, offering its users a flexible, valuable, socially compelling tool. Its users are the ones ghost riding the privacy whip, dancing around on the roof as they expose their personal information to the world."[1050] Grimmelman therefore argues in favor of an educational approach which specifically targets users of social networking sites in an effort to help understand the risks associated with the exposure of their personal information.

Even so, the usage and retention of personal information, provided by users to Facebook, by Facebook is a topic of heated discussion. Especially the original ability to delete an account proved problematic for users.[1051] Facebook only provided users with the ability to deactivate the account rather than complete deletion. The alternative for users was to individually delete each profile element. Facebook responded to the criticism and eased the account deletion procedure for users wanting to part with the social networking site.[1052] Other problems nevertheless continued since Facebook 'shares' information received from users with third parties. This occurs when users install Facebook applications or gadgets. Adrienne Felt and David Evans write how "[w]hen Jane installs a Facebook application, the application is given the ability to see anything that Jane can see. This means that the application can request information about Jane, her friends, and her fellow network members. The owner of the application is free to collect, look at, and potentially misuse this information."[1053] The Canadian Internet Policy and Public Interest Clinic (CIPPIC) filed a complaint against Facebook in 2008 alleging 22 separate violations of Canadian privacy law.[1054] These violations included Facebook's failure to inform users of how Facebook discloses their personal information to third parties for advertising and other profit-making activities, and Facebook's failure to obtain permission from its users for such uses and disclosures of the personal information of its members.[1055] The user outrage did not occur until the following year when Facebook made changes to its terms

---

[1048] *Ibid.*

[1049] Grimmelman, J. (2009). Saving Facebook. *Iowa Law Review*, Vol. 94: 1137-1206.

[1050] *Ibid:* 1140.

[1051] The Information Commissioner's Office (ICO) in the United Kingdom commenced an investigation into Facebook in 2008 after the ICO received a complaint from a user about the inability to delete the account. See Vallance, C. (2008). Facebook faces privacy questions. Available at: http://news.bbc.co.uk/2/hi/technology/7196803.stm (last accessed July 13, 2010).

[1052] Still problems exist since account deletion does not automatically lead Facebook to also delete groups created by the deleted users.

[1053] Felt, A. & D. Evans (n.d.). Privacy Protection for Social Networking APIs. Available at: http://www.cs.virginia.edu/felt/privacy/ (last accessed July 13, 2010).

[1054] Canadian Internet Policy and Public Interest Clinic (CIPPIC) (2008). CIPPIC files privacy complaint against Facebook. Press release, May 30, 2008. Available at: http://www.cippic.ca/uploads/NewsRelease_30May08.pdf (last accessed July 13, 2010).

[1055] *Ibid.*

of service which led to increased media attention about the practices of the social networking site.[1056] Facebook changed the terms of service and deleted a provision which allowed members to remove their content at any time. Moreover, the new language added to the terms of service stated how Facebook would retain the content and licenses of users even after they terminated their accounts.[1057]

More problems began to accumulate for Facebook when the website decided to engage in a round of changes to its privacy policies. The Electronic Privacy Information Center (EPIC) filed a Federal Trade Commission (FTC) complaint when Facebook redefined much of the information provided by its members as 'publicly available information.'[1058] Facebook responded to the criticism and announced how "[i]n the coming weeks, we will add privacy controls that are much simpler to use. We will also give you an easy way to turn off all third-party services."[1059]

The importance of the current dispute over Facebook and its treatment of the information provided by its members is the distribution of responsibility with respect to the 'exposure' of personal information. The line between consumer as opposed to business facilitation becomes blurry and this in turn also influences the judgment about the 'facilitator.' For if perpetrators obtain the information from a third party which said third party obtained from a Facebook profile page, who facilitates? This is an important argument in particular because consumer awareness primarily focuses on this type of consumer facilitation, the voluntary information dispersion. From the 'old fashioned' method of dumpster diving to the more innovative method of perusing social networking sites, the argument goes that perpetrators cleverly take advantage of both the 'carelessness' and the 'cluelessness' of consumers. This is certainly the area over which consumers have a sense of 'control' and an area in which consumer awareness may at least have some success. This category indicates how, especially as consumers become more knowledgeable about the dangers present in contemporary society, there is at least some room for improvement with regard to reducing consumer facilitation. In contrast, the subsequent two categories begin to demonstrate a shift with regard to consumer control and the level of voluntary involvement on the part of consumers.

6.2.2 Social Engineering

When consumers do not provide the information voluntarily or unprompted, perpetrators themselves have to hunt for it. And they have managed to do so rather well. In contemporary society, phishing has become a well-known concept, especially among those involved in various areas related to digital technology. The underlying principle of phishing, which is gaining personal information through social engineering techniques, is far from new. As Hiep Dang notes, "[w]hether it's called social engineering, trickery, confidence tricks, cognitive biases, or scams, the concept of exploiting a person's naivety and trust is as prevalent today as it has

---

[1056] Stelter, B. (2009). Facebook's Users Ask Who Owns Information. *New York Times*, February 16, 2009.
[1057] *Ibid.*
[1058] See http://epic.org/privacy/facebook/
[1059] Zuckerberg, M. (2010). From Facebook, answering privacy concerns with new settings. *Washington Post*, May 24, 2010.

been since the dawn of time."[1060] The craft of the con artist has always been present and used for a variety of criminal activities. Before the Internet domination, perpetrators used more traditional means such as calling and ringing doorbells trying to obtain valuable information. Kevin Mitnick, one of the most 'infamous social engineers' in the modern era, carefully outlines how con artists used more 'old-fashioned' social engineering techniques, such as calling, to obtain valuable information from businesses.[1061] Through the art of persuasion, con artists successfully managed to convince employees of various corporations to surrender pivotal business information, including passwords.[1062] The ultimate art used by perpetrators is to convince the target, whether a business or a consumer, that they are someone else, someone trustworthy. The Internet provided and continues to provide perpetrators with the ideal platform to update their old techniques and to more efficiently target consumers. The variety of ways perpetrators incorporated social engineering techniques on the Internet is rather impressive, even during the early days. Special Agent Riley described how "[o]ne of the most popular things to do to get people to give up their personal information is to offer credit card accounts at a very, very low interest rate, such as 4.9 or 5.9 percent."[1063] Perpetrators developed websites to offer credit card accounts in search of personal information. Riley offers another example when she describes how "[i]n addition to the credit card applications themselves, several others of the schemes that are available out there right now include credit rescue operations where pages, again, using very high-quality graphics are made to look legitimate and offer the ability for you to wipe out any credit problems you have simply, again, by providing all of your personal financial information."[1064] Especially during the early days of the Internet, consumer awareness about potential fraud schemes was severely absent. Perpetrators gratefully managed to take advantage of this absence.

The first actual phishing 'attacks' differed greatly from their current counterparts. The term phishing entered the circuit in 1996 when hackers managed to get unsuspecting America On-line (AOL) users to reveal their passwords. With their passwords, the hackers could gain free internet access. Since then, phishing has become an attractive profit making strategy for various individuals involved in financial identity theft. The online banking system became a source of revenue for perpetrators. Especially consumers in the United States proved both an easy and an attractive target due to universality of the English language and the one-factor authentication system most often used for online banking. Phishing emails sent to Dutch consumers, on the other hand, appeared suspicious from the start. In particular, an infamous email sent by perpetrators posing as the Postbank, formerly one of the main Dutch banks. The phishing emails sent in name of the Postbank made the mistake of using the opening *Lieve Postbankklant*, which directly translates into "Dear Postbankclient," except the dear used in the phishing emails is reserved for letters written to close friends and loved

---

[1060] Dang, H. (2008). The Origins of Social Engineering. *McAfee Security Journal*: 8.
[1061] Mitnick, K., Simon, W. & S. Wozniak (2002). *The art of deception: controlling the human element of security*. Indianapolis, IN: John Wiley & Sons.
[1062] *Ibid.*
[1063] Riley, M. (1998). Statement to the U.S. Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary. *The Identity Theft and Assumption Deterrence Act*, Hearing, May 20, 1998 (Serial 105 - 779): 7.
[1064] *Ibid:* 8.

ones. Furthermore, the email mainly uses the informal "you" (*je*), similar in German *du* and in Spanish *tu* as opposed to the more formal and more appropriate *u*, or in German *Sie* and Spanish *usted*, which is a direct sign that there is something out of the ordinary going on. The initial attack led some clients to click on the link and as such the bank was forced to replace usernames, passwords and TAN codes. This also occurred in other European countries. As Dirro & Kolberg note, "[i]n the early days, messages were composed in a crude German notation that looked like it was an English or a Russian text translated by Babel Fish. That's probably what happened."[1065]

As information on phishing attacks began to grow, perpetrators also expanded and sophisticated their methods. Ram Dantu *et al.* describe how the nature of phishing attacks changed over time.[1066] Whereas initial attacks were passive such as password guessing and eavesdropping, more recent attacks are active through the employment of Trojans, traffic interception, and the adoption of social engineering techniques. The introduction of phishing as a vehicle to commit financial identity theft led to research on consumer behavior and phishing detectability.[1067] Both academic and non-academic researchers aimed to analyze the awareness of consumers with regard to phishing attacks and their ability to recognize phishing emails. Rachna Dhamija *et al.* conducted a usability study to determine which phishing strategies proved successful.[1068] The best phishing website managed to fool 90% of the participants through its incorporation of padlock in content, Verisign logo and certificate validation seal, and a consumer alert warning. As the authors note, "…the indicators of trust presented by the browser are trivial to spoof. By using very simple spoofing attacks, such as copying images of browser chrome or the SSL indicators in the address bar or status bar, we were able to fool even our most careful and knowledgeable users."[1069] This is a crucial development with regard to consumer facilitation and the perception held by society about such facilitation. The media, along with policy makers and business professionals, often refer to popular research conducted by, for example, Javelin Strategy & Research.[1070] Javelin concluded how consumer awareness of phishing is high. Such a conclusion paints a deceiving picture of the relationship between phishing awareness and consumer ability. Basically, through proclaiming a high consumer awareness of phishing, Javelin allows the remainder of society to believe consumers can resist the phishing threat. And have the means to do so. This is a misleading conclusion. Awareness may be high but actual ability to detect a phishing email, especially of the sophisticated kind, appears low as indicated by Dhamija *et al.*[1071]

Overall, perpetrators have successfully managed to eliminate many of the early pitfalls including sloppy language and overly obvious signs of unprofessional

---

[1065] Dirro, T. & D. Kolberg (2008). Germany: Malware learns the language. *Sage*, January 2008: 27.
[1066] Dantu, R., Palla, S. & J. Cangussu (2008). Classification of Phishers. *Journal of Homeland Security and Emergency Management*, Vol. 5 (1): 1 – 14.
[1067] Jakobsson, M. (2007). The Human Factor in Phishing. *Privacy & Security of Consumer Information '07*. Available at: http://www.informatics.indiana.edu/markus//papers/aci.pdf (last accessed July 13, 2010).
[1068] Dhamija, R., Tygar, J. D. & M. Hearst (2006). Why Phishing Works. *Proceedings of the Conference on Human Factors in Computing Systems*.
[1069] *Ibid:* 9.
[1070] Javelin Strategy & Research (2005b). *Phishing: Consumer Behavior and Awareness*. Syndicated Report Brochure.
[1071] Dhamija, Tygar & Hearst (2006).

communication. Instead, they currently manage to imitate businesses and other organizations to the point that they can fool many, if not most, consumers. Dantu *et al.* acknowledge how "[t]he major factors in any phishing attack are forgery and social engineering. No matter how many authentication techniques we develop, phishers always adapt."[1072] Others, however, disagree. Michael Barrett states how he believes "...phishing is a completely preventable crime when you combine technology with education. Our anti-phishing efforts with Yahoo over a 10 month period prevented more than 85 million phishing emails from ever reaching the intended victim. And if we can teach end users some simple rules, it will have a big impact."[1073] Xun Dong *et al.*, on the other hand, reject the value of user education as a means to 'prevent' successful phishing attacks or to solve the problem.[1074] This rejection is based on the awareness of Dong *et al.* that "...to discover the mismatches when metadata is spoofed requires extra tools and knowledge which most users simply don't have and should not be expected to have. It is the system designers' responsibility to ensure information displayed on the user interface is resistant enough against most spoofing attacks, especially the meta-data."[1075] Others recognize value in user education, but criticize the ways through which such education is currently administered.[1076]

6.2.3 'Involuntary' Facilitation

The increased sophistication of phishing proved to be a foreshadowing of a progression into the 'involuntary' state of consumer facilitation. The incorporation of social engineering techniques still heavily relied on the voluntary participation of consumers to surrender their personal information. Such reliance is far from desirable for perpetrators. As a result, perpetrators managed to develop means to benefit from consumer facilitation without the need for their active participation. While previously introduced methods have not disappeared, the turn to sophisticated methods of involuntary and passive facilitation certainly influences the means, or lack thereof, of consumer control. As Jennifer Lynch notes, "...recent phishing attacks have become more sophisticated and involve technological devices that may be beyond the ken of even relatively savvy consumers. Some of these attacks, such as those that automatically change a recipient's hostfile, do not even require any action to be taken by the consumer, so she would be hard-pressed to educate herself on how best to protect herself from this type of attack."[1077] The main drive behind involuntary consumer facilitation is the presence of botnets. According to various authors, botnets have become the

---

[1072] Dantu, Palla & Cangussu (2008): 4.
[1073] Qtd. in Georgia Tech Information Security Center (2009). Emerging Cyber Threats Report 2009. Available at: http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf (last accessed July 13, 2010): 8.
[1074] Dong, X., Clark, J. A., & J. Jacob (2008). Modelling User-Phishing Interaction. *2008 Conference on Human System Interactions*: 627-632.
[1075] *Ibid:* 630.
[1076] See for example Harley, D. & A. Lee (2007). Phish Phodder: is User Education Helping or Hindering? *17th Virus Bulletin and Conference Proceedings*; Martin, T. (2009). Phishing for Answers: Factors Influencing a Participant's Ability to Categorize Email. Available at: http://projects.csail.mit.edu/spamconf/SC2009/Tim_Martin/Martin_Phishingv2.doc (last accessed July 13, 2010).
[1077] Lynch, J. (2005). Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks. *Berkeley Technology Law Journal*, Vol. 20: 278.

largest security threat in contemporary society.[1078] Phillip Hunter explains how "[i]ndeed one of the reasons for the botnet becoming the number one security threat lies not in the innovation of its method of recruitment or attack, but in its resistance to defence."[1079] Other authors echo similar concerns.[1080] Its other main attractive feature is its speed. Botnets are "...networks of infected end-hosts, called bots, that are under the control of a human operator commonly known as botmaster. While botnets recruit vulnerable machines using methods also utilized by other classes of malware…their defining characteristic is the use of command and control (C&C) channels."[1081] Through these channels, the botmasters can send out commands to their 'botarmies.' The creation of botarmies is surprisingly easy. Nicholas Ianelli & Aaron Hackworth describe how creating a botnet only requires minimal technical skill.[1082] This is predominantly a result of the assistance of the underground community. The community is more than willing to share its vast knowledge through a variety of channels. Seasoned perpetrators, for example, provide training sessions and advice to newcomers through Internet Relay Channels (IRC).[1083] Through the spread of knowledge, seasoned perpetrators can assist in the increasing growth of botnets around the world. The growth leads to a greater challenge for detecting and subsequently taking down botnets.

Botnets have various goals which fall into three categories, information dispersion, information harvesting and information processing. With regard to financial identity theft, information harvesting and information dispersion are the most relevant goals. Julian B. Grizzard *et al.* describe how "…information dispersion includes sending out spam, creating denial of service attacks, providing false information from illegally controlled sources, etc. The goal of information harvesting includes obtaining identity data, financial data, password data, relationship data (i.e., email addresses of friends), and any other type of data available on the host."[1084]

Botmasters create botarmies through the deployment of malware. Perpetrators can manipulate the installation of malware through a variety of channels. They can seduce consumers into downloading an executable file through, for example, a phishing attack or they can send the malware along with another download. More recently, perpetrators have introduced even more undetectable and more involuntary means of installing malware. As Niels Provos *et al.* note "[i]n most cases, a successful exploit results in the automatic installation of a malware binary, also called *drive-by-download*. The installed malware often enables an adversary to gain remote control over the compromised computer system and can be used to steal sensitive personal information such as banking passwords, to send out spam

---

[1078] See for example Hunter, P. (2008). PayPal, FBI and others wage war on Botnet armies. Can they succeed? *Computer Fraud & Security*, Vol. 2008: 13 – 15.

[1079] *Ibid:* 13.

[1080] Brand, M., Champion, A. & D. Chan (2007). Combating the Botnet Scourge. Unpublished paper. Available at:
http://www.cse.ohio-state.edu/~champion/research/Combating_the_Botnet_Scourge.pdf
(last visited July 2, 2010).

[1081] Abu Rajab, M., Zarfoss, J., Monrose, F. & A. Terzis (2006). A Multifaceted Approach to Understanding the Botnet Phenomenon. *Proceedings of ACM SIGCOMM/USENIX Internet Measurement (IMC)*: 41.

[1082] Ianelli, N. & A. Hackworth (2007). Botnets as a Verhicle for Online Crime. *The International Journal of Forensic Computer Science*: 19 – 39.

[1083] *Ibid.*

[1084] Grizzard, J. B., Sharma, V., Nunnery, C. & B. B. Kang (2007). Peer-to-Peer botnets: Overview and Case Study. Paper presented at *Usenix Hotbots 2007*: 3.

or to install more malicious executables over time."[1085] Drive-by-downloads are dangerous because detection of such downloads is extremely difficult for consumers. As such these attacks are a significant threat and deserve considerable attention. Through the drive-by-download, perpetrators manage to install malware, which can include keyloggers. These keyloggers function much like cameras and capture all information typed into the computer. This makes the collection of personal information easy and convenient for perpetrators of financial identity theft. Especially, since consumers are most likely unaware of the presence of a keylogger since its installation via the drive-by-download also occurred without the knowledge of the consumer. The data obtained via keyloggers is subsequently transferred to dropzones. These dropzones are publicly writable directories on an Internet server which serves as an exchange point for keylogger data.[1086] Important to note, is how "[c]ontrary to conventional wisdom, the malicious pages weren't mostly hosted on the seedier parts of the internet such as adult and gambling websites. While there were a large number of drive-by infections on adult sites, the majority of the malicious data is hosted on sites whose categorisation is more mundane such as finance, home and garden, and business."[1087] According to Chengyu Song *et al.*, drive-by downloads are currently one of the most severe threats for users on the Internet. Moreover, such downloads are presently the number one malware vector.[1088] According to Frei *et al.*, "[t]he tip of the Web browser insecurity iceberg was measured to be 637 million (or 45.2%) Internet users at risk worldwide due to not running the latest most secure browser version. Meanwhile, hidden below the surface, the iceberg extends further encompassing users that rely on outdated vulnerable browser plug-ins."[1089] This is a disturbing statistic, especially since drive-by downloads target these browser plug-ins.[1090] The main challenge is to focus on the individual yet bear in the mind the individual's 'inability' or rather limited ability to conquer the most advanced threats to information security.

6.3 Conclusion

What is happening is a shift in various aspects of consumer facilitation. In previous years, perpetrators appeared to benefit from the 'carelessness' or 'cluelessness' of consumers. Especially those individuals who would toss out

---

[1085] Provos, N., McNamee, D., Mavrommatis, P., Wang, K. & N. Modadugu (2008).The Ghost In The Browser Analysis of Web-Based Malware. Available at: http://www.usenix.org/event/hotbots07/tech/full_papers/provos/provos.pdf (last accessed July 13, 2010): 1.

[1086] Holz, T., Engelberth, M. & F. Freiling (2008). Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones. Available at: https://www.fehcom.net/fh-frankfurt/vorlesungen/2008_WS/itsec/material/impersonation-attacks-TR.pdf (last accessed July 13, 2010).

[1087] Potter, B. (2008). How bad is it? *Network Security*, Vol. 2008: 19.

[1088] Song, C., Zhuge, J., Han, X. & Z. Ye (2010). Preventing Drive-by Download via Inter-Module Communication Monitoring. *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*: 124 -134.

[1089] Frei, S., Duebendorfer, T., Ollman, G. & M. May (2009). Understanding the Web browserthreat: Examination of vulnerable online Web browser populations and the "insecurity iceberg." ETH Zurich Tech Report Nr. 288: 9.

[1090] Egele, M., Wurzinger, P., Kruegel, C. & E. Kirda (2009a). 'Defending Browsers against Drive-by Downloads: Mitigating Heap-spraying Code Injection Attacks,' in U. Flegel & D. Bruschi (eds.) *Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer: 1 – 19.

important documents without in some way destroying the personal information exposed. Basically, perpetrators benefited from the unprompted availability of personal information. As financial identity theft, however, moved into the online realm it appears as though perpetrators smelled the opportunity to hunt for personal information, without running a high risk of getting caught. This allowed them to gain more control over which information they obtained and from whom.

There is a subsequent movement from voluntary and active to involuntary and passive consumer facilitation. This movement, demonstrated through the continuous evolution of methods used by perpetrators and detected by those trying to counter the problem indicates a diminishing dependability on actual consumer actions. 'Old-fashioned' methods are certainly still in circulation, but the expansion of opportunities allows especially the sophisticated criminals to carry out their operations with the most advanced methods. These perpetrators find an easy 'in' and they can manage to do everything themselves from there on out. Botnets immaculately reflect this current state of affairs. These botnets have become the epitome of involuntary and passive consumer facilitation, especially through the introduction of 'drive-by downloads,' which are according to various sources among the most common methods for spreading malware these days.[1091] Whereas with phishing emails, consumers received a prompt to release personal information in an active manner, perpetrators have managed to eliminate this need for active consumer involvement through the introduction of drive-by downloads. The lack of active consumer involvement means consumers facilitate aspects of financial identity theft without actually having the ability to prevent such facilitation. This is a vital aspect to bear in mind with respect to the overall opportunity structure of financial identity theft, especially in light of countermeasures and the potential for their effectiveness. Certain sources appear to neglect the ability factor when they write "[w]e must realize that we are the front line of defense against cybercrime; we must understand that our carelessness could facilitate a successful cyberterrorist or information warfare attack on the critical infrastructures of our society."[1092] This is not about carelessness anymore. Perpetrators have now managed to place their entire operation outside of the reach of consumers, which makes the act of crime repression, let alone prevention, far more challenging. The technological sophistication of current operations requires significant background knowledge which even the savviest consumers often do not posses. They, along with their instruments such as their computers, are used without their knowledge or influence. This movement creates more challenges because old band-aids such as awareness campaigns start to become less valuable; yet, the consumer remains a primary target for perpetrators of financial identity theft, especially on the electronic superhighway and as such requires attention.

[1091] See for example *Ibid.*

[1092] Brenner, S. W. & L. L. Clarke (2005). Distributed Security: A New Model of Law Enforcement. *SSRN Accepted Papers Series*: 17.

7 | The Others

The result of nearly any categorization is a category which groups the left-overs together and calls them 'others.' This is a familiar concept for survey research, where questionnaires inquire about the participants' age, ethnicity, income, etc. and generally provide a category labelled 'others.' The group of 'others' often consists of misfits who fail to claim membership of another category. The appealing aspect of the 'others' is the gathering of diverse actors. This, however, complicates the establishment of overarching conclusions about this category. Certain actors included in this chapter demonstrate considerable overlap with other actors covered in previous chapters, whereas other actors included demonstrate a unique position and original means of facilitation with respect to financial identity theft. This chapter is not comprehensive for all of the possible members of the 'others' category. Instead it aims to capture the most significant and influential others in relation to the facilitation of financial identity theft. Elucidating the facilitation of the 'others' besides the main actors of the previous chapters is essential to complete the picture of the opportunity structure of financial identity theft.

7.1 Information Brokers

7.1.1 United States

The events of September 11, 2001 and the subsequent 'War on Terror' increased their popularity[1093], but information brokers soared long before then. Mark D. Seltzer notes how "[t]he seemingly inexhaustible demand for financial information, once thought to be confidential and regulated, has spawned a multi-million dollar industry of information brokers."[1094] These information or data brokers are private corporations which make it their sole business to collect, analyze, and sell personal information. In many ways, their presence and value represent the embodiment of the information society. Derek J. Somogy describes how the information and computer industry developed in a parallel fashion. The private sector began to digitize and subsequently store marketable information in searchable databases during the 1970s. These developments led to an increase of demands and capacities with respect to the computer industry. As a result, the scope and the amount of digital information available for sale also increased.[1095] Data brokers, or information resellers, jumped in to take advantage of the new market opportunity. The market value of the industry increased during the beginning of the twentieth century when the backlash of September 11th placed a 'premium value on accurate identification'[1096] of individuals in the public as well as

---

[1093] Brooks, N. (2005). *Data Brokers: Background and Industry Overview*. Congressional Research Service (CRS) Report to Congress.
[1094] Seltzer, M. D. (1999). The New Threats to Financial Privacy: Is there Liability for Financial Institutions and Their New Antagonists, the Information Brokers? *Boston Bar Journal*, Vol. 43: 8.
[1095] Somogy, D. (2006). Information Brokers and Privacy. *I/S: A journal of Law and Policy*, Vol. 2 (3): 904.
[1096] Brooks (2005).

the private sector. The prosperity of data brokers is partially a result of their usefulness with regard to the law enforcement community. This is due to the ability of data brokers to "...maintain and organize personal information on individuals in a manner that may not be legally available to government actors."[1097]

Despite their value to various actors in both the public and the private sector, data brokers remained out of the public eye for a long time. Like an invisible shadow the brokers conducted their core activities of obtaining, processing and selling personal information, without any interference. This all changed when the media discovered and subsequently reported on several major security breaches. Suddenly, the spotlight illuminated all of the vulnerabilities data brokers exposed individuals to while conducting every day business. These data breaches form the core source of information for the analysis of facilitating factors contributed by data brokers. Important to note is how the link between data obtained from data brokers and financial identity theft is difficult to establish (see chapter 3) but has been done in a number of cases, most notably ChoicePoint.

As a result, ChoicePoint is a relevant object of analysis to examine the role of information brokers in the facilitation of financial identity theft. ChoicePoint is one of the largest data brokers currently operating in the United States and caters its information selling services to three different markets. These include business, insurance, and government agencies.[1098] In order to serve these different markets, ChoicePoint maintains significant amounts of sensitive personal information. Data security breaches began to plague ChoicePoint as a result of this. The most famous and most damaging data security breach came in 2004.[1099] In October of that year, law enforcement officials notified ChoicePoint about the ways in which individuals within an 'identity theft ring' used the data broker to obtain sensitive personal information.[1100] Perpetrators posed as legitimate clients and opened accounts to access personal information held and sold by ChoicePoint. As Robert O'Harrow describes, "ChoicePoint Inc. electronically delivered thousands of reports containing names, addresses, Social Security numbers, financial information and other details to people in the Los Angeles area posing as officials in legitimate debt collection, insurance and check-cashing businesses."[1101] Research following the discovery indicated a total of 50 fake corporations had been set up and registered with ChoicePoint to accumulate personal information of unsuspecting citizens.[1102] Several months later, in February 2005, MSNBC was the first to break the news and several newspapers followed up on the ChoicePoint breach.

The Federal Trade Commission (FTC) began its investigation against ChoicePoint shortly after the breach came to light. In its formal complaint, the FTC notes how ChoicePoint ultimately notified 163,000 consumers about the data security breach and how "[i]n all cases, the information disclosed by ChoicePoint included unique identifying information that facilitates identity theft, such as dates of birth and Social Security numbers, as well as nearly 10,000 credit reports. At

---

[1097] *Ibid:* 2.

[1098] Electronic Privacy Information Center (EPIC) (n.d.). ChoicePoint. Available at: http://www.epic.org/privacy/choicepoint/ (last accessed July 13, 2010).

[1099] O'Harrow, R. (2005). ID Data Conned from Firm. *Washington post*, February 17, 2005: E01.

[1100] Sullivan, B. (2005). Database giant gives access to fake firms: ChoicePoint warns more than 30,000 they may be at risk. Available at: http://www.msnbc.msn.com/id/6969799/ (last accessed July 13, 2010).

[1101] O'Harrow (2005): E01.

[1102] Sullivan (2005).

least 800 cases of identity theft arose out of these incidents."[1103] The fact that perpetrators managed to obtain 'unique identifying information' puts the affected consumers at risk of becoming victims of true name fraud, because the perpetrators obtained sufficient information to open new accounts. The FTC's complaint against ChoicePoint mainly focuses on the company's failure to recognize the illegitimate nature of some of their clients and their businesses. According to the FTC, "...applications contained false credentials and other misrepresentations, which ChoicePoint failed to detect because it had not implemented reasonable procedures to verify or authenticate the identities and qualifications of prospective subscribers."[1104] More specifically ChoicePoint accepted proofs of identification which, according to the FTC, were clearly fraudulent or at least demonstrated the applicant was clearly not a legitimate business. The FTC provides a plethora of examples about inadequate applications including critical information left blank, conflicting business addresses, information which indicated businesses were suspended or inactive, and utility statements demonstrating delinquent accounts. Furthermore, ChoicePoint's own internal reports linked at least one applicant to possible fraud associated with the Social Security number of another individual.[1105]

In addition to the inaccurate way of verifying the identities of prospective clients, ChoicePoint continued its line of mistakes and its facilitation of potential identity theft cases when it failed to recognize rather suspicious account activity. ChoicePoint provided a relatively large number of consumer reports to 'a purported apartment leasing subscriber', which significantly exceeded the total number of apartments owned by the subscriber, over a rather short period of time.[1106] Furthermore, ChoicePoint disregarded obvious red flags such as a disconnected phone line, incorrect business addresses, use of stolen credit card numbers, and payments exclusively made through money orders which all indicated possible fraud; yet, ChoicePoint continued to provide this particular subscriber with various consumer reports. According to the FTC, ChoicePoint also failed to monitor the accounts of certain suspicious subscribers, even after it received subpoenas from law enforcement agencies which alerted it to the presence of fraudulent accounts.[1107]

The problem with the ChoicePoint data security breach then is two-fold. The first and primary problem is the inability or unwillingness of ChoicePoint to implement adequate means to verify the identity of prospective clients. The underlying motive could have been the exclusive focus on speed and customer convenience rather than an increased effort to ensure the legitimacy of potential clients and their requests in order to ensure that unique personal information of citizens does not end up in the hands of criminals. This sounds strikingly familiar to the vulnerabilities exposed in the application process of financial service providers for prospective clients (see section 5.2.1). The second problem, which simply enhances the first and the scope at which perpetrators can manage to carry out their activities, is ChoicePoint's way of monitoring accounts.

[1103] *United States of America* v. *ChoicePoint* (2006). Supplemental stipulated judgment and order for permanent injunction and monetary relief: 4.
[1104] *Ibid.*
[1105] *Ibid:* 6.
[1106] *Ibid.*
[1107] *Ibid.*

The exposure of ChoicePoint and its business practices also attracted the attention of the United States Congress. The breach strengthened the rekindled criticism of the information privacy framework in the United States, and certain sources of criticism even came accompanied by concrete proposals for improvement.[1108] The tribute of the ChoicePoint data security breach is the exposure of vulnerabilities of the information brokerage industry. Whereas certain sources[1109] previously recognized the dangers, others appeared in the dark about the industry as well as its practices and potential connection to financial identity theft. The increased pressure generated by all publicity led ChoicePoint to begin implementing enhancements to its privacy and information security framework. Such enhancements include the establishment of an Office of Privacy, Ethics and Compliance to reinforce the responsible use and protection of information at ChoicePoint through such means as policies and procedures, audit and compliance, and outreach and education.[1110]

The publication of the ChoicePoint data security breach proved to be the tip of the iceberg, as later media stories demonstrate. The media needed to divide its attention as another breach found its way into the spotlight in 2005. LexisNexis, another major data broker, has aggregated news, business, and legal documents for a long time, but in 2005 LexisNexis acquired Seisint, which resells public records to law enforcement and private investigators. During the same year, LexisNexis found itself unfavorably presented in the media after a large data security breach. In total, the broker notified at least 310,000 individuals whose personal information may have been compromised.[1111] The perpetrators in this case started out their activities through sending massive amounts of infected emails. Brian Krebs reported how "...a police officer in Florida was among those who opened the infected e-mail message. Not long after his computer was infected with the keystroke-capturing program, the officer logged on to his police department's account at Accurint, a LexisNexis service provided by Florida-based subsidiary Seisint Inc."[1112] Through logging on, the police officer provided the perpetrators with the necessary information to continue their operations. The group used the police department's name and billing information to create a series of new accounts, which helped them to access more data on a larger scale. Additionally, Kurt P. Sanford, President and Chief Executive Officer of LexisNexis, also indicated how insider theft, where LexisNexis employees illegally obtained consumer data, accounted for part of the data security breach. On September 19, 2008 ChoicePoint became a LexisNexis company and aided in the expansion of LexisNexis as a data emporium.

ChoicePoint and LexisNexis are merely two examples of information brokers who experienced data security breaches. The exposure of the breach came as a

---

[1108] See Solove, D. J. & C. J. Hoofnagle (2006). A Model Regime of Privacy Protection. *University of Illinois Law Review*, Vol. 2006 (2): 357 – 404.

[1109] The Electronic Privacy Information Center (EPIC) acknowledged the problems associated with the information brokerage industry, especially ChoicePoint many years prior to the actual breach.

[1110] Privacy Rights Clearinghouse (2010). Chronology of Data Breaches Security Breaches 2005-Present. Available at: http://www.privacyrights.org/data-breach (last accessed July 5, 2010).

[1111] LexisNexis (2005). LexisNexis Concludes Review of Data Search Activity, Identifying Additional Instances of Illegal Data Access. Press Release. Available at: http://www.lexisnexis.com/about/releases/0789.asp (last accessed on July 5, 2010).

[1112] Krebs, B. (2005). Computers seized in data-theft probe. *Washington Post*. May 19, 2005. Available at: http://www.washingtonpost.com/wp-dyn/content/article/2005/05/19/AR2005051900704.html (last accessed July 5, 2010).

result of the pioneering data security breach notification law in California (see chapter 3). During the last several years, data security breaches, whether in the public or the private sector, have become comfortably familiar in the United States. As the spread of data security breach notification legislation indicated in chapter 3, the majority of States have responded to the problem. When the Identity Theft Task Force composed its strategic plan in 2007, the Force described how "[i]dentity thieves, however, can steal personal information from data brokers who fail to ensure that their customers have a legitimate need for the data."[1113] The first stage of financial identity theft, therefore, can be greatly facilitated by the presence and subsequent practices of the information brokerage industry.

7.1.2 The Netherlands

The industry of data brokers in the Netherlands is limited and rather distinct in comparison to the United States. There are list brokers in the Netherlands. These list brokers are private corporations who maintain addresses of potential clients. These addresses are attractive for other corporations for marketing purposes in an effort to approach and subsequently obtain more clients. Listbokers 'rent' the addresses of prospective clients to the corporations.[1114] This means that corporations do not actually obtain the information. Instead the list brokers forward the marketing materials to prospective clients and when such recipients of the materials respond, the corporation manages to obtain their addresses.[1115]

Other types of businesses which fall into the category of information brokers are information agencies or *informatiehandelbureaus*. Despite their lack of overt publicity, the potential for problems with this type of business certainly exist. Several years ago, in August 2001, the Registration Chamber, the predecessor of the Data Protection Authority (DPA), conducted an investigation into the business practices of a particular information marketing agency. In the introduction of its investigation, the Registration Chamber acknowledges how information agencies operate in a legal grey area. This is because there is a clear societal need for information about credit defaulters yet simultaneously information collection about these defaulters is also subject to privacy and data protection restrictions. Investigations into the business practices, in particular the methods of information collection, had previously (in 1996[1116] and 1999[1117]) been conducted by the Registration Chamber. These investigations included announced visits to examine the methods used for information collection by the agencies and to investigate whether such practices coincided with the previous Data Protection Act.[1118]

The in 2001 published investigation, which began in 2000, came after the Registration Chamber received several complaints during the previous years, from 1998 to 2000. These complaints came from citizens and various organizations who received information inquiries from a specific information agency. Citizen complainants indicated how representatives of the information agencies had

---

[1113] Identity Theft Task Force (2007). *Combating Identity Theft: A Strategic Plan.*
[1114] Schermer, B. W. & T. Wagemans (2009). *Onze digitale schaduw. Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat.*
[1115] *Ibid.*
[1116] Handelsinformatiebureau X.
[1117] Goderie van Groen.
[1118] Registratiekamer (2001). *Onrechtmatige handelwijze van een handelsinformatiebureau.*

approached neighbors and family members to obtain information about them without their permission. Similar complaints came from organizations operating in both the public and the private sector such as health insurance corporations, municipal social services, and the office for government unemployment benefits.[1119] When the Registration Chamber confronted the information agency with the complaints, the agency claimed others must have used its name in an effort to collect information from these organizations. Based on the complaints and the response provided by the agency itself, the Registration Chamber decided to begin an investigation.

In its conclusions, the Registration Chamber notes how the information agency was aware of the confidentiality mandate of the sources the agency approached but still neglected this knowledge in an effort to acquire confidential information. When certain organizations refused to provide such information and referred to their confidentiality mandate, the information agency placed them on a do not contact list for future assignments. Others still remained eligible for inquiries. Certain internal documents found at the information agency's office described how employees were allowed to make up information if such false stories allowed them to acquire the necessary information from the contacted sources.[1120] Defaulters, whose information is being collected by the information agency, are put under pressure when they refuse to cooperate in the information collection activities.

Moreover, the information agency turned out to have regular access to the automated system of a large government benefit database. The previous investigations conducted by the Registration Chamber also demonstrated how information agencies engaged in illegal information collection practices. A similar case returned when the DPA office received a complaint about company X and the DPA began an investigation.[1121] Initially, the DPA sent written questions to company X and found the answers to develop sufficient grounds for further action. This occurred via an unannounced visit at the business location of company X. The DPA reserves the legal authority to conduct such unannounced visits for investigation purposes. The DPA wanted to develop a judgment about the modus operandi of the company in order to determine its compliance with the Dutch Data Protection Act.

The DPA determined how company X primarily caters its services to law offices, insurance companies, and the banking sector.[1122] Other clients include process servers (bailiffs), debt collection agencies, and investigation agencies. The main request from clients for company X is to retrieve the credit worthiness of an individual and also her bank account number along with the account balance. In a tender to a law office, company X describes how for its special research the company aims to discover the real estate value of individuals as well as information about their income. Moreover, the company also conducts large scale bank investigations to determine the account balances of the individuals. This includes checking and savings accounts, as well as stock portfolios. All of this information is used by the clients of company X to determine whether seizure of property is a viable option. Company X maintains standard prices for its services.

[1119] *Ibid.*
[1120] *Ibid.*
[1121] College Bescherming Persoonsgegevens (CBP) (2003). *Onrechtmatig, onbehoorlijk en onzorgvuldig. De verwerking van persoonsgegevens door een handelsinformatiebureau voor rapportage van verhaalsinformatie.*
[1122] *Ibid.*

For bank account information, for example, Company X charges 60 euros and a criminal background check costs 350 euros.

Through the DPA's investigation of the documents obtained during the unannounced visit, it became clear how company X proved successful in its delivery of the services mentioned above.[1123] To obtain such information company X uses various sources. These include outsourcing the requests to private investigation agencies, research by its own employees via interviews or neighborhood research, and also 'calling rounds.' Basically employees from company X call various agencies, both public and private. These include social services, healthcare insurance companies, the tax administration office, banks, the municipal administrative office, and others. Furthermore, company X also uses regular contact persons who have access to address information, social-fiscal numbers, and background check information. Other sources of information used by company X include open or public sources.

Based on its investigation, the DPA came to several important conclusions about the business practices of company X. The information collection practices of company X violate data protection legislation in the Netherlands, since company X fails to demonstrate a necessary legal mandate to collect such information. Moreover, the DPA concludes how there is a lack of evidence which demonstrates permission from the party in question for company X to collect such personal information. The DPA furthermore determined how company X does not contact the party in question nor is there any evidence of an agreement between the party in question and company X. Company X also failed to follow the notification procedures as identified in the Dutch Data Protection Act which require organizations to inform the DPA of its information collection and processing activities.

The most worrisome development is the ability of company X to obtain information from sources which are under a legal mandate to maintain the information in a confidential manner. Company X manages to obtain such information predominantly through social engineering and the DPA managed to locate specific conversation strategies which demonstrate how employees of company X used false names and employers to obtain confidential information from (mainly) government sources. The DPA describes how company X knew or should have known how certain sources are under a legal or professional obligation to maintain the confidentiality of the information which company X requested.

Other violations include the manner in which company X keeps its records stored. During the initial written questions filed by the DPA, company X provided false information and claimed how the company destroyed all information of a party in question after the case closed. The investigation of the DPA, however, revealed how company X maintains a database both electronically and physically which contains the previously compiled reports.

Overall, the investigation of the DPA demonstrates the problematic aspect of the business practices of company X, and the industry of information agencies, but also the ease of accessibility to information from sources which maintain the obligation to keep such information confidential.[1124]

[1123] *Ibid.*
[1124] *Ibid.*

The various investigations conducted by the Registration Chamber and its successor the DPA spread demonstrate how information agencies obtain and process their information in an unlawful manner. This is problematic, but important to bear in mind is how information agencies generally turn to the public sector to acquire the necessary information. This leads to the development of an overall image which assumes that for potential perpetrators of financial identity theft government agencies may generally form a more attractive target to facilitate the first stage of financial identity theft. They may use information agencies as an intermediary, but this seems far less likely than in the United States, where the industry itself actually maintains an important place in the information market.

7.2 Payment Processors

Besides information brokers, other sources also spark the interest of potential perpetrators of financial identity theft. Due to the involvement of multiple parties, the chain of a credit card transaction is complex. A credit card transaction can require the involvement of five different parties.[1125] These include the client, the merchant, the 'issuing' bank, the 'acquiring' bank, and the credit card company. The 'issuing' bank is the bank where the client maintains her credit card, whereas the 'acquiring' bank refers to the bank of the merchant. The actual credit card process involves all of these parties. The client starts the process through the purchase with a credit card. The merchant verifies the authenticity of the credit card either electronically or via the telephone to determine whether the credit card is valid and sufficient funds are available to complete the purchase. When the issuing bank returns with a positive response, the merchant can complete the purchase and the client receives the product. After the completed purchase, the credit limit of the client is adjusted by the issuing bank but the merchant has not received its money. This occurs at the end of the day, when the merchant collects all credit card purchases and sends them to the credit card company.[1126] The credit card company in turn ensures the clearing and settlement of the transactions between the issuing and the acquiring bank. The credit card data of the clients which the merchant sends to the credit card company are the object of desire for perpetrators of financial identity theft. Since certain portions of the transaction and the data processing might be outsourced to third parties the already complex chain is complicated even further. These third parties are the payment processors.

7.2.1 United States

At the start of 2009, Heartland Payment Systems became the center of attention after its public declaration of a data security breach which occurred during the previous year. News stories captured the announcement and the breach became one of the largest ever.[1127] The discovery of the breach came after Heartland began to receive fraudulent activity reports from MasterCard and Visa. The credit cards had all been used at merchants who use Heartland for the processing of its

---

[1125] Le Comte, M. (2009). Een groeiende golf van credit card frauds. Een kwestie van pompen, verzuipen of een dam bouwen? *Bank- en Effectenbedrijf*, July/August 2009: 14 – 18.
[1126] *Ibid.*
[1127] Krebs, B. (2009). Payment Processor Breach May Be Largest Ever. *Washington Post*. Available at: http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html (last accessed July 5, 2010).

customer payments.[1128] Heartland contacted the United States Secret Service after the discovery of the breach. The source of the breach turned out to be "[a] piece of malicious software planted on the company's payment processing network that recorded payment card data as it was being sent for processing to Heartland by thousands of the company's retail clients."[1129] The Heartland breach once again led to a demonstration of the necessity for even better information security.[1130]

The Heartland breach was not first breach which caught widespread media attention. Several years earlier, in 2005, Cardsystems experienced a similar fate. On May 23, 2005 Mark Perry, CEO of Cardsystems, notified the Federal Bureau of Investigations (FBI) about a data security breach, which, after investigation, exposed the information of 40 million card holders. Perry notes how, "…an unauthorized party placed a script (a sequence of instructions interpreted or carried out by another program) on the CardSystems platform (an underlying computer system on which application programs run) through an internet-facing application that is used by our customers to access data. This script ran on our system and caused records to be extracted, zipped into a file, and exported to an FTP site (similar to a web address). It was a sophisticated script that targeted a particular file type, and was scheduled to run every four days."[1131] Perry goes on to explain how forensic investigations demonstrated that there was only one confirmed instance, on May 22, 2005, where data was actually exported. The script specifically searched CardSystems computer servers for records which contained track data (the data retained on the magnetic stripe of a credit card). The most complete information any perpetrator could have gathered, according to Perry, about cardholders includes the individual's name, account number, expiration date and CVV code (contained in the magnetic stripe). Furthermore, Perry claims that considering the track data does not include social security numbers of the affected consumers, identity theft is virtually impossible. Account takeover, however, appears very possible.

These breaches are merely two prominent examples which have occurred during the last several years. Both, however, provide two important observations. First, payment processers are an attractive target for perpetrators of financial identity theft, since these processors maintain large amounts of sensitive financial information. The second aspect which surfaces based on a brief overview of the two breaches is the technological sophistication of the attacks. This illustrates how perpetrators manage to make significant progress throughout the years to advance their attacks in terms of technological sophistication, which complicates prevention and detection. This strengthens the trend which was already observed in the analysis of the consumer in chapter 6.

7.2.2 The Netherlands

In the Netherlands, the industry of payment processors is tremendously influenced by the developments within the European Union. The introduction of

---

[1128] *Ibid.*

[1129] *Ibid.*

[1130] Cheney, J. S. (2010). *Heartland Payment Systems: Lessons Learned from a Data Breach.* Discussion Paper Payment Cards Center, Federal Reserve Bank of Philadelphia.

[1131] Perry, J. M. (2005). Statement to the U.S. House Subcommittee on Oversight and Investigations of the Committee on Financial Services. *Credit Card Data Processing: How Secure is it?* Hearing, July 21, 2005 (Serial 109 – 48): 4-5.

the Single Euro Payments Era (SEPA) led to the anticipation of increased competition among payment processors in the European Union. This anticipation led to the development of the largest pan-European payment processor, Equens. Equens came about through a merger between the Dutch Interpay and the German 'Transaktionsinstitut für Zahlungsdienstleistungen' (TAI) during the fall of 2006. The Dutch Interpay had been in existence since 1994 and was brand name owner of several payment products including the PIN, Acceptgiro, Incasso, and Chipknip. In 2003, Interpay began to focus on the European market as a result of the introduction of the Euro and the internationalization of the bank and business sector. Due to this shift in focus, Interpay began to reduce its involvement in certain activities and the brand name ownership of the payment products was transferred to another corporation, Currence. This is when Interpay began to exclusively focus on payment processing and expanded its business through the merger with the German corporation and the establishment of Equens.

News about breaches occurring at Equens appear unavailable. Instead, Equens is a key actor in the fight against skimming and credit card fraud in the Netherlands. For over a year, Equens has incorporated a mixture of techniques, including working with neutral networks, in an effort to reduce the financial damage caused by skimming.[1132] These techniques lead to extremely fast detection.[1133] In May 2010, a cooperative effort of Equens and the *Vrije Universiteit* of Amsterdam led to the development of a method to decrease skimming in the Netherlands.[1134] Equens, as a result, appears to primarily play a role in prevention rather than facilitation of financial identity theft.

7.3 Merchants

The acceptance of various payment products, especially the credit card, in both the physical and the virtual world makes merchants a relevant actor to examine with respect to the facilitation of financial identity theft. Whereas in the physical world merchants face challenges in the usage of payment products, through the identity authentication of the owner of the payment product, these challenges are exacerbated by the developments in the virtual world, as a result of the lack of face to face contact. The introduction of e-commerce changed the landscape for businesses and consumers around the globe. The ability to purchase and sell goods and services regardless of location or business hours proved to be an attractive idea for both parties. The existence of economic incentives through cost reduction and creation of innovative means of additional revenue added to the popularity of e-commerce for various actors in society.[1135] Despite its popularity, e-commerce still faces challenges. The altered landscape introduced additional and more complicated vulnerabilities for abuse which translate into opportunities for perpetrators of financial identity theft. This potential for abuse certainly influences the popularity of e-commerce applications for consumers. Chapter 6 provided an

---

[1132] De Vrede, T. (2010). Equens bestrijdt skimmen met computerkracht. *Automatiseringgids*. Available at: http://www.automatiseringgids.nl/artikelen/2010/21/equens-bestrijdt-skimmen-met-computerkracht.aspx (last accessed July 5, 2010).

[1133] *Ibid.*

[1134] *Ibid.*

[1135] Strader, T. J. & M. J. Shaw (1997). Characteristics of electronic markets. *Decision Support Systems*, Vol. 21.

exposition of the various threats consumers presently face on the Internet. The main focus herein is on the mechanism implemented to verify the identity of the client who conducts the purchase. The distinction between the United States and the Netherlands is perhaps less relevant for this actor since consumers can access e-retailers from anywhere in the world. Nevertheless, the United States and the Netherlands maintain diverse methods of payment for sites or stores which originate in both countries.

7.3.1 United States

The usage of credit cards in the physical world in the United States proved problematic since merchants generally only authenticated the credit card rather than the owner of the card. This meant the mere possession of the card proved sufficient for perpetrators of financial identity theft to conduct purchases in the name of the actual owner of the card. Since the Truth in Lending Act capped the liability costs of credit card owners at 50 dollars the actual damage to the owners remained limited. This also provided credit card issuers with the liberty to maintain a system which continued to potentially facilitate financial identity theft. Throughout years, credit card issuers did make changes such as the inclusion of photographs of the owner on the card. Yet, the actual ability to authenticate the owner rather than just the credit card remained with the merchant. Since the credit card issuer was absent during the actual transaction. Merchants in the United States have introduced changes for credit card transactions, albeit in a fragmented fashion. Certain stores request to see a driver's license of the client in order to verify the identity whereas others actually compare the signature on the back of the card as compared to the signature on the receipt.

Since the popularity of the credit card in the United States extended into the virtual world, so did the accompanying vulnerabilities. The majority of e-retailers which originate in the United States accept credit card payments through the Internet. From amazon.com to other online websites of stores, credit cards provide an efficient and convenient method of payment via the Internet for both consumers and businesses. Through the use of the credit card, neither the consumers nor the businesses needed to transfer to another system, which meant additional costs remained out of sight. The problem with the transfer of the credit card from the physical to the virtual world is well-documented. For the underground market began to target credit card numbers and subsequently use them to purchase goods and services in the name of the victim. This consequence is the result of an underestimation of the challenges posed by e-commerce payment transactions. [1136] The transition from the physical to the virtual world failed to translate into a transition of security for the credit card. The financial services sector initially designed the credit card for the physical world and as such the instrument proved ill prepared for the virtual world.

The e-commerce sector began to respond to the challenges posed by payment transactions in the virtual world. At first, e-retailers began to request the CVC code printed on the back of the credit card. Since the underground market predominantly traded in credit card numbers without the accompanying CVC code, this measure managed to cover part of the problem. To access the CVC

[1136] Heng, S. (2004). *E-Payments: Modern Complement to Traditional Payment Systems*. Deutsche Bank Research, Economics Working Paper 44.

code, clients needed to physically possess the credit card. Even so, this measure became familiar to perpetrators of account takeover and these perpetrators began to provide credit card numbers with CVC codes through the underground market. Moreover, through the use of malware perpetrators also manage to obtain all information inserted onto the screen which means they can obtain the CVC code as well.

The rat race continued when the financial services industry returned with other alternatives to increase security, but also to transfer the liability of fraudulent transactions from the e-retailers onto the financial service provider. This is a crucial aspect of the incentives for both the financial service providers and e-retailers to become involved in the development of increased security for e-commerce transactions. The Truth in Lending Act states how consumer liability for fraudulent transactions carried out by credit cards is capped at a maximum of 50 dollars. As a result, consumers who contact their credit card company in light of a fraudulent transaction receive a refund. Whereas consumers receive the money back via their credit card company, retailers or in this case e-commerce businesses must refund the financial loss to the credit card company. This is due to chargeback liability, which basically states that when a consumer disputes a credit card transaction and the credit card issuer sides with the consumer the retailer must return the money. This occurs under the rules promulgated by the Federal Reserve.[1137] The chargeback liability means that even if the retailer did nothing 'wrong' it must still bear the liability for the costs incurred as a result of the fraudulent transaction. Due to the burden imposed as a result of the chargeback liability, retailers would logically display an interest in the prevention of fraudulent payments via the Internet; yet, the opposite appears true. Todd Pearson noted how "...there is little value in being an early adopter and incurring the high costs associated with implementing fraud-reduction software without a shift in the liability for chargebacks."[1138] As a result, the financial services industry began to offer alternatives which aimed to improve security and provide retailers with the shift of liability if they subscribed to the 'system.' Visa introduced its Verified by Visa (VbV) system on April 1, 2003. As Visa notes, "[a] liability shift for any participating Merchant protects them against a cardholder denying making the purchase. Therefore, VbV results in a reduction in chargebacks and disputes, together with a reduction in the related operational costs. The merchant benefits from this protection even when the Issuer or cardholder is not participating."[1139] Jeff King acknowledges the contribution of VISA, and Mastercard, which introduced a similar system called Mastercard Secure Code, and claims they have been on a crusade to train retailers to practice good security techniques.[1140]

Despite the 'good will' displayed by Visa and Mastercard, the e-commerce business still feeds the bill through its participation to the program which requires them to enroll. There are benefits for the retailer because of the shift of liability; yet, the system also carries the necessary costs in order to ensure such a shift.

[1137] Furletti, M. (2004). *Prepaid Card Markets & Regulation*. Discussion Paper Payment Cards Center.

[1138] Sienkiewicz, S. & M. Bochicchio (2002). The Future of E-Commerce Payments. Available at: http://www.phil.frb.org/payment-cards-center/events/conferences/2002/FutureECommerce_062002.pdf (last accessed July 5, 2010).

[1139] VISA (n.d.). Verified by Visa: Merchant fact sheet. Available at: http://www2.visaeurope.com/documents/vbv/verifiedbyvisa_merchantfactsheet.pdf (last accessed July 14, 2010).

[1140] Wales, E. (2003). E-commerce counts cost of Online Card Fraud. *Computer Fraud & Security*, Vol. 2003 (1): 9-11.

Moreover, the actual security offered by the system is difficult to assess, which is irrelevant for the retailers since their primary aim is to eliminate the costs associated with the chargeback liability, but relevant for consumers and the facilitation of financial identity theft. On its site Visa notes how "[t]he 3-digit security code shown on the back of your Visa card lets merchants know that you're physically holding the card when you make a purchase online or over the phone. It's yet another layer of protection Visa implements to prevent fraud before it happens."[1141] Once entered, however, this code can easily be captured by malware which provides perpetrators of financial identity theft with the code.

7.3.2 The Netherlands

The description of the credit card in chapter 5 already demonstrated its limited popularity in the Netherlands, and for the e-commerce business the same situation seems to apply. In stores in the Netherlands, the majority of clients appear to pay for purchases either through cash or through their debit card which always requires the input of a PIN code. This still provides for opportunities of criminal conduct as the popularity of skimming has indicated. For the e-commerce realm, the methods of payment offered to consumers in the Netherlands appear more diverse than in the United States. The majority of e-commerce businesses in the Netherlands grant consumers the option to pay via their credit cards. Yet, consumers can also make an order and request the bill to be send along with the product.

The charm of multiple options also came accompanied by disadvantages for Thuiswinkel.org[1142] which claimed the existence of various options leads to chaos. Several years ago, in 2004, Thuiswinkel.org spoke of a state of financial disorder on the Internet with regard to payment methods. Back then, Thuiswinkel.org certainly made a valid point since retailers themselves decided which methods of payment they wanted to accept and which they cared to reject. This led to inconsistent practices and confusion for consumers. This ultimately inspired iDeal. Since 2005, iDeal is the Internet banking payment standard which is developed by various Dutch banks. iDeal directly connects the consumer to her bank online and allows a transfer to be made to the particular e-commerce business, so that the security methods for online banking apply (see section 5.4.2). As a result, the consumer directly pays for the good or service. The introduction of iDeal synchronized the method of verification of clients, since retailers use the online banking system. This leads to a synchronization of challenges and benefits. The danger of MITM attacks against online banking therefore transfers onto the online stores as well. Overall, 47 per cent of transactions occur through the iDeal payment system.[1143]

Thuiswinkel.org is actively involved and actually refers to the need to pay attention to the issue of identity theft.[1144] For credit card payments conducted via

---

[1141] VISA (n.d.). 3-Digit Security Code. Available at: http://usa.visa.com/personal/security/visa_security_program/3_digit_security_code.html (last accessed July 14, 2010).

[1142] Thuiswinkel.org is the representative organization for e-retailers in the Netherlands.

[1143] Reijerman, D. (2010). Thuiswinkel.org wil dat meer webwinkels 3D Secure gaan gebruiken. Available at: http://tweakers.net/nieuws/67644/thuiswinkel-punt-org-wil-dat-meer-webwinkels-3d-secure-gaan-gebruiken.html (last accessed July 13, 2010).

[1144] Werkgroep Betalingsverkeer Nederlandse Thuiswinkel Organisatie (2010). *Position Paper Online betalen in Nederland.*

the Internet, Thuiswinkel.org encourages and stimulates the usage of the 3D secure system as described above.[1145] The director of the organization emphasizes the transfer of liability from the retailer onto the credit card company. This is especially important since just as their American counterparts, e-retailers in the Netherlands also suffer from the rules surrounding chargeback liability. While already half of all e-retailers in the Netherlands have joined the system, the director aims to stimulate all of them to join.[1146] There appears to be resistance to the implementation of the system by remaining e-retailers since the additional means of authentication also increases the number of actions the consumer must take to complete a transaction. Since the 3D secure system is inconsequential in the instruments (a self selected password, a pin code, or a randomizer) used for the increased security, e-retailers fear consumers shall be surprised by the 3D secure prompt and cancel the transaction.[1147] This yet again demonstrates the contested relationship between convenience and security, where an increase in security leads to a decrease in convenience and as such to the potential loss of clients. Moreover, the working group of the representative organization also recognizes how credit card issuers have failed to update the previously identified security problems with the original 3D secure system.[1148] Despite the relatively small percentage of transactions which occur through credit card payments (9 per cent), the damage caused to e-retailers through credit card payments is estimated to be in the tens of millions of euros a year by Thuiswinkel.org.[1149] Other sources, such as the Dutch Central Bank and the individual banks refuse to provide indications of the financial damage caused through credit card fraud due to the fear of potential damage to consumer trust in the system.[1150] Thuiswinkel.org therefore continues to encourage the usage of iDeal since according to the organization payments via credit cards provide more space for perpetrators of financial identity theft to engage in man in the middle attacks, since the e-retailer must conduct the identification of the client rather than the bank. The iDeal payment system after all relies on identification of the client through the Internet banking system, which includes its relatively high level of security in comparison to the credit card system.

7.4 Internet Service Providers

The main purpose of an Internet Service Provider is to provide its clients with access to the Internet. Yet, Internet Service Providers can also function as host provides for content on websites. In both functions, Internet Service Providers play a unique role with respect to the facilitation of financial identity theft. This dual purpose of providing access and serving as a content host illustrates the importance of Internet Service Providers in the overall opportunity structure of financial identity theft. This is especially due to the significance of Internet access for perpetrators of financial identity theft. To gain such access is vital, but perpetrators of the crime also need a host for their activities, such as phishing websites. The exclusive position of Internet Service Providers with respect to

---

[1145] Reijerman (2010).
[1146] *Ibid.*
[1147] Werkgroep Betalingsverkeer Nederlandse Thuiswinkel Organisatie (2010).
[1148] *Ibid.*
[1149] *Ibid.*
[1150] Weissink, A. M. J. (2010). Cyberbende koopt staatsloten. *Het Financiële Dagblad.* June 1, 2010.

security in the virtual world forces them to stand in the spotlight. This also leads to a discussion about the role and the responsibility that Internet Service Providers ought to have. Tyler Moore and Richard Clayton capture the complexity when they write, "[i]t is impractical for Internet Service Providers (ISPs) to police the entirety of the content that their users place upon the Internet, so it is generally seen as unjust for ISPs to bear strict liability, viz: that they become legally liable for the mere presence of unlawful content."[1151] On the other hand, "…the ISPs are in an unrivalled position to suppress content held on their systems by removing access to resources – webspace, connectivity, file access permissions, etc. – from their customers."[1152] Others instead gravitate toward the outer skirt of the problem. Several years ago, in 2004, Doug Lichtman and Eric Posner proclaimed how Internet Service Providers "..are today largely immune from liability for their role in the creation and propagation of worms, viruses, and other forms of malicious computer code."[1153] This is not entirely true for Internet Service Providers operating in the European Union, since the Directive on e-commerce states "…service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities."[1154] According to Lichtman and Posner, they join a "growing chorus of legal commentators" who all argue in favor of increased accountability and responsibility for Internet Service Providers. The reason for such an increase in accountability and responsibility is to develop incentives for Internet Service Providers to improve security. The assumption in the argument of Lichtman & Posner therefore revolves around a lack of inherent incentives for Internet Service Providers to invest in security. This assumption is also found in other sources. The United Kingdom House of Lords Science and Technology Committee stated in 2007 how "…although ISPs could easily disconnect infected machines from their networks, there is no incentive for them to do so."[1155] The Committee instead claims how "…there is a disincentive, since customers, once disconnected, are likely to call help-lines and take up the time of call-centre staff, imposing additional costs on the ISP."[1156] Others echo similar notions. Jennifer A. Chandler writes "[t]he parties best placed to address cyber insecurity, including…ISPs…do not face the full consequences of their contributions to cyber insecurity. Accordingly, they do not invest time and money to the socially optimal level of improved security."[1157] Chandler claims Internet Service Providers, along with selected other actors, fail to experience the negative consequences of cyber insecurity which leads to lack of incentives to act rather than to remain passive. Yun Huang *et al.* state this proposition in more general terms when they write "…the parties that suffer the most are not in the best

---

[1151] Moore, T. & R. Clayton (2008). The Impact of Incentives on Notice and Take-down. *Workshop on the Economics of Information Security (WEIS):* 1.
[1152] *Ibid.*
[1153] Lichtman, D. & E. Posner (2004). Holding Internet Service Providers Accountable. University of Chicago Law & Economics Working Paper: 2.
[1154] Directive 2000/31/EC.
[1155] House of Lords: Science and Technology Committee (2007) Personal internet security: 5th report of session, Vol. 1: Report: 30.
[1156] *Ibid.*
[1157] Chandler, J. A. (2006). Liability for Botnet Attacks. *Canadian Journal of Law and Technology*, Vol. 5 (1): 21.

position to defend, while the parties in the best position do not suffer enough to defend."[1158]

Michel J. G. van Eeten en Johannes M. Bauer call the argument about a lack of incentives on the side of Internet Service Providers into question. Internet Service Providers may, according to van Eeten and Bauer, "…unwittingly reinforce the impression that they have few if any incentives to improve the security of their services."[1159] This occurs through the resistance of Internet Service Providers to government intervention and the hesitance to surrender self-regulation. The resistance to government intervention is interpreted by many as an unwillingness to provide more security; yet, this is an incorrect conclusion according to van Eeten and Bauer. Based on interviews with officials from Internet Service Providers, the authors develop ample evidence to demonstrate both the efforts made by the providers and also unravel the incentives behind these efforts. These efforts began to escalate around 2003 when Internet Service Providers began to understand how improved security turned out to be in their best interest. This is due to costs associated with insecurity of their clients. These costs come from 'security-related' customer calls. As van Eeten en Bauer note, "[t]he incentive here is that security incidents generate customer calls, thus quickly driving up the costs of customer care."[1160] There are other incentives. These include costs associated with brand and reputation damage, and infrastructure expansion.

In addition to 'negative' or cost dominated incentives, 'positive' or benefit oriented incentives also play a role in the decision to engage in improved security. According to van Eeten and Bauer, all interviewees mentioned the benefits generated through maintaining reciprocity. This refers to the contacts maintained with other Internet Service Providers, CSIRTS and other related organizations, who can provide assistance during a case. Such assistance and contact is reciprocal, but to maintain such reciprocity Internet Service Providers must treat complaints of abuse seriously. As van Eeten and Bauer conclude, "[t]he more abuse takes place on its network, the more other contacts in the network will ask for intervention."[1161] This, in turn, enforces security since threats from other Internet Service Providers provide a powerful incentive for the 'threatened' Internet Service Provider to improve security.

There appear to be sufficient incentives for Internet Service Providers, at least those of a reputable nature to invest in cyber security. Still complications surface. Based on the responses offered to the Arbor Network's fifth annual 'Worldwide Infrastructure Security Report' (WWIR), a year long industry-wide operational security survey, Danny McPherson drew the following conclusion "…while attackers increasingly and successfully monetise DDoS, phishing and other illegal activities, many providers report struggles with budget and management support for security initiatives and investment."[1162] As a result, McPherson notes how a growing concern about a range of innovative threats has managed to replace any optimism on the site of the Internet Service Provider. In response to the survey,

---

[1158] Huang, Y., Xianjun, G., & Whinston, A. (2007). Defeating DDoS attacks by fixing the incentive chain. *ACM Transactions on Internet Technology*, Vol. 7 (1): 1 – 19.

[1159] van Eeten, M. J. G. & J. M. Bauer (2008). *Economics of Malware: Security Decisions, Incentives and Externalities*. STI Working Paper 2008/1: 26.

[1160] *Ibid*: 27.

[1161] *Ibid:* 30.

[1162] McPherson, D. (2010). Cybercrime - A game of cat and mouse in 2009. *Network Security*, Vol. 2010 (2): 18.

one provider notes how "the bad guys are beating us, badly."[1163] This is a worrisome development especially in light of the crucial position Internet Service Providers hold with respect to the facilitation of financial identity theft. Access to the Internet is a vital instrument for the successful completion of a financial identity theft operation. For without the Internet, many of the activities carried out as part of the identity theft operation, such as obtaining the relevant personal information along with the ability to drain accounts, conduct fraudulent transactions, and transfer money would not be possible in such a low risk and convenient manner. Moore *et al.* also underscore the prominent place Internet Service Providers can play in detection and how "ISPs are also uniquely placed to limit the external impact of an infected computer: they control its Internet connection and can disconnect it if need be. Current best practice is less drastic: it is to quarantine infected computers into a 'walled garden' subnetwork from which they can access decontamination and software patches but not much else."[1164] McPherson also states therefore how many providers reflected on the need for better cooperation and coordination between both providers and vendors to meet the future Internet security challenges.[1165]

The great diversity of Internet Service Providers in the United States may also complicate matters. As Moore *et al.* recognize "[t]he approximately 4,000 ISPs in the United States range in size from mom-and-pop firms serving a few hundred customers in rural outposts to behemoths such as AT&T, Verizon, AOL, and Comcast, which each provide online connectivity to millions of households and businesses."[1166] Whereas the large Internet Service Providers maintain the resources and staff to engage in detection and clean up of infected machines, the smaller providers lack such an ability.

7.5 Money Mules

The paper trail established through the fight against money laundering (see also chapter 5) also provides a challenge for perpetrators of financial identity. To circumvent the paper trail, perpetrators of financial identity theft solicit the assistance of money mules. The purpose of money mules is to use their bank account to accept the illicit funds and to transfer them to another account. As Brian Krebs notes, "[m]ule recruitment is an integral part of many cyber crime operations because money transferred directly from a victim to an account controlled by criminals is easily traced by banks and law enforcement. The mules, therefore, serve as a vital buffer, making it easier for criminals to hide their tracks."[1167] As such, mules decrease the risk of getting caught and losing the proceeds of the crime. Money mules are different from all other parties previously considered for they are not actors but rather characters. Much like in a play individuals take on the role of the money mule. According to Ken Durham, money mules "...are individuals unwittingly hired by organized criminals to

---

[1163] Qtd. In *Ibid.*

[1164] Moore, T., Clayton, R. & R. Anderson (2009). The Economics of Online Crime. *Journal of Economic Perspectives*, Vol. 23 (3): 9 - 10.

[1165] McPherson (2010).

[1166] Moore *et al.* (2009): 9.

[1167] Krebs, B. (2008). 'Money Mules' Help Haul Cyber Criminals' Loot. *Washington Post*. January 25, 2008. Available at:
http://www.washingtonpost.com/wp-dyn/content/story/2008/01/25/ST2008012501460.html
(last accessed July 13, 2010).

perform international wire fraud and other illicit operations."[1168] Durham describes mules indirectly as innocent or rather as indirect victims of organized criminals who are unaware of the illicit aspect of the operation. This is a one-sided representation of money mules, for some may be unaware but certainly not all. As Krebs notes, "I have interviewed more than 150 money mules in the course of my investigations over the last year into this type of fraud. I can safely say that most mules fit into one of two camps: Those that are simply not the sharpest crayons in the box and really did get bamboozled (at least up to a point); and those who are out of a job, laid off, or otherwise in need of money and simply aren't asking themselves or anyone else too many questions about the whole process."[1169] Krebs furthermore states how most mules actually fit into the latter group. The individuals who fall into the latter category generally set up a different bank account to use aside from their original checking account. "When pressed as to why they did this, if they're honest most will say they weren't sure about the whole arrangement and wanted to protect their investments just in case their employers turned out to be less-than-honest."[1170]

Even so, there appears to be a grey area especially when mule recruitment approaches candidates in desperate need of a job. Krebs describes the story of Deena Monroe, an unwitting money mule. Monroe, a single mother who had just been laid off as a warehouse supervisor, received a job offer through her email. The company found her resume through careerbuilder.com and offered a work-from-home position in the sales department of a marketing company in Australia. Monroe stated that she researched the company before accepting the offer. The company first asked her to add an additional e-mail address to her PayPal account, which was necessary for her to transfer money on the company's behalf. Krebs describes how "[s]oon after, Monroe received a deposit of $2,601 into her PayPal account, with instructions to transfer the money to her checking account, withdraw it and wire the bulk of the amount via Western Union to two separate addresses in India. She was told to keep 10 percent as her commission."[1171] Problems started less than two weeks later when an eBay user emailed Monroe asking her when he would receive the new computer he had won and purchased for $2,601 at the auction. EBay became involved and concluded how the fraudulent company, also known as Monroe's employer, used her PayPal account for a fake auction. EBay held Monroe responsible for the 'stolen' funds and she had to repay the auction 'winner.' Unawareness about organized crime operations, as a result, can lead to the victimization of unintentional accomplices.

More general information on money mules appears limited. A clear perspective on the number of money mules currently engaged in criminal operations seems unavailable. Yet, sporadically certain statistics do surface. According to the Australian High-Tech Crime Centre, "[i]n January 2005, 61 people were arrested in Australia for allegedly wiring money to Russia and other undisclosed locations and collecting a commission based on the amount of money laundered. Mules reportedly earned $200 – $500 per day for moving up to $100,000 per day."[1172]

[1168] Durham, K. (2006). Money Mules: An Investigative View. *EDPACS*, Vol. 33 (8): 13 – 19.
[1169] Krebs, B. (2010). FBI Promises Action Against Money Mules. Available at: http://krebsonsecurity.com/2010/05/fbi-promises-action-against-money-mules/ (last accessed July 13, 2010).
[1170] *Ibid.*
[1171] Krebs (2008).
[1172] Australian Institute of Criminology (2007). Money Mules. *High Tech Crime Brief.*

According to statistics provided by the Dutch Banking Association in 2010, there were 1400 'young victims' of bank fraud who functioned as money mules.[1173] These money mules are viewed as victims because of the repercussions associated with their cooperation in the criminal operation. Once the bank discovers the involvement of the mule, the bank demands a return of the funds from the mule and places the mule on a black list. This black list implies that the mule cannot open an account, buy a house, or apply for a loan during the following eight years.

In the majority of literature, the presence and role of money mules is mentioned in passing without any insightful details about the incidence rate. Yet, this is also a particularly challenging task to carry out, since many money mules manage to successfully accomplish their task in the overall criminal operation. And as a result, if this is the case, many financial service providers may be unwilling to share the information publicly for fear of reputation damage. According to Kelly Jackson Higgins, money mule recruiters have managed to take advantage of the present economic crisis. As Higgins notes, "[a]s the unemployment rate has climbed, so has the amount of money-mule recruitment and job-related spam scams that prey on people losing their jobs. Job-related spam campaigns jumped 514 percent between August and October when the economic crisis first began to unfold, according to new data released by Panda Labs, including data gathered from The Project Honeypot. Even more disturbing is that seven of the world's largest money-mule crime networks have been able to successfully dupe their victims into moving their stolen money or assets 30 percent of the time, according to research from Panda Labs."[1174]

While the main red thread throughout this research focuses on the facilitation of the first and the second stage of financial identity theft, the money mule plays a vital role in the facilitation of the third stage of the crime. This third stage liquefies the proceeds which allows the perpetrators to actually obtain the financial assets generated through the crime. Money mules are therefore an essential aspect for perpetrators of financial identity theft to successfully complete the criminal operation.

7.6 Conclusion

The 'others' depict distinct stories. For the facilitation of the first stage of financial identity theft, information brokers and payment processors are lucrative targets for perpetrators of the crime. The attacks carried out against both actors, through the media stories on data security breaches, illustrate how the sensitive information maintained by both is wanted by perpetrators. As a result, information brokers and payment processors exacerbate an existing vulnerability with respect to the availability and accessibility of personal information, which facilitates the first stage of financial identity theft. Especially the proliferation of the information brokerage industry demonstrates the increasing vulnerability both the public and the private sector expose citizens to due to their information obsessive needs. Such needs manage to feed the information brokerage industry, at least in the United States.

[1173] Dinjens, M. (2010). Banken: Aantal slachtoffers van bankfraude ligt veel hoger. *Metro*, June 24, 2010: 3.

[1174] Higgins, K. J. (2008). Recruitment of Unwitting Money Mules on the Rise. Available at: http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=212101088 (last accessed July 13, 2010).

For the Netherlands, the industry appears to cater to a smaller market and remains limited in terms of scale. Even so, the practices of information collection by these information agencies are questionable and in turn demonstrate the potential vulnerability of information exposure by those with a mandate to keep such information confidential, namely government agencies.

Merchants are a key player during the second stage of financial identity theft, where perpetrators aim to misuse the previously acquired payment product or information. The e-commerce boom increased the pressure for improved means of identity authentication. Such an improved means is attempted through the 3D secure system but remains uncertain with respect to its effectiveness. In the Netherlands, the iDeal option comes accompanied by a *higher* level of authentication due to the reliance of the payment option on the two-factor authentication system used for Internet banking activities. This usage of a previously existing system, however, also comes accompanied by the same vulnerabilities to the Man in the Browser Attack (see section 5.4.2).

For perpetrators of financial identity theft to carry out fraudulent transactions and to acquire personal information, access to the Internet is a vital tool. Internet access also increases the pool of suitable targets and decreases the risks associated with getting caught. This leads to the prominent role played by Internet Service Providers, who provide individuals with access to the Internet and can serve as host providers. In this sense, Internet Service Providers can facilitate both the first and the second stage, as their contribution to the opportunity structure is overarching. As became apparent, however, Internet Service Providers generally maintain prime incentives to improve security and attempt to keep illegal content removed from the Internet.

Unlike the other actors, money mules are unique since they facilitate the rarely discussed third stage of financial identity theft. To actually profit from the proceeds, perpetrators of financial identity theft recruit money mules to circumvent audit trails. Such money mules therefore play a role in decreasing the risks associated with transferring money away from the victim's account. As such, mules are important intermediaries within the overall operation to successfully obtain the proceeds of the crime.

In contrast to the roles played by information brokers, payment processors, and merchants, therefore, Internet Service Providers and money mules are unique in their role as which enhances their importance in the facilitation of financial identity theft.

8 | From Piece to Puzzle

The idea of a jigsaw puzzle is a suitable metaphor for the problem of financial identity theft. The previous five chapters provide an in-depth and detailed overview of the individual pieces of the puzzle, or rather the facilitating factors of financial identity theft. This chapter, in contrast, takes a step back to observe the entire puzzle, or the broad picture, in an effort to develop an opportunity structure. Ronald V. Clarke uses the notion of a crime opportunity structure to demonstrate the interdependent relationship between crime opportunity and a variety of societal aspects.[1175] These include socio-economic structure, including demographics and geography, as well as lifestyle/routine activity and physical environment. All of these aspects influence the core of the crime opportunity structure which contains the victims, targets, and facilitators. Since the opportunity structure takes a comprehensive approach to the social context of crime, its construction for financial identity theft must contain both the overarching features of all facilitating factors as well as an understanding of the underlying mechanisms which nurture them. This is precisely why the usage of the process tracing approach was appropriate to gain valuable background information on the underlying mechanisms which established the (potential) facilitating factors as well as the process of facilitation of financial identity theft itself.

8.1 Opportunity Structure of Financial Identity Theft

8.1.1 Information: Abundance, Availability, Accessibility

Information is everywhere and provided by everyone. This is, after all, the information society. This abundance of information is mainly the result of the developments made in the field of digital technology. Various aspects of information collection and processing which hindered the massive character of such activities in the physical world are no longer an obstacle in the virtual world. The exponential growth of information storage capacity has been closely followed by the amount of information stored, processed, and shared. This in turn also came accompanied by the escalating importance of information in contemporary society, especially as the Internet began to play a more prominent role in daily routine activities. The importance of information in the information society therefore is apparent. This importance has transformed information itself into a hot product.[1176] Clarke developed the idea of hot products and used the following acronym to describe its criminogenic attributes: CRAVED. This acronym stands for Concealable, Removable, Available, Valuable, Enjoyable and Disposable. Hot products do not necessarily embody all of these attributes in a similar way and variations of degrees certainly exist, as Clarke and Newman recognize.[1177] Information certainly has the ability to embody all of these attributes, but

---

[1175] Clarke, R. V. (1995). 'Situational Crime Prevention,' in M. Tonry & D. P. Farrington (eds.) *Building a Safer Society: Strategic Approaches to Crime Prevention*. Chicago: University of Chicago Press: 103.
[1176] Newman, G. R. & R. V. Clarke (2003). *Superhighway Robbery: Preventing e-commerce crime*. Willian Publishing.
[1177] *Ibid.*

especially its value and availability have developed it into a hot product.[1178] Information, according to Newman & Clarke, is a prime ingredient found in all products of e-commerce and this ingredient is therefore often the target of crime in the virtual world. This finding is directly transferable to the realm of financial identity theft, for information is a prime ingredient for perpetrators to carry out their activities. This is apparent since the acquisition of information is the first stage of any financial identity theft operation. As a result, much emphasis throughout the previous chapters is placed on information and its abundance, availability, and accessibility.

The abundance of information is in part a response to the perception of such information accumulation as a means to reduce risks and uncertainties.[1179] According to Richard V. Ericson and Kevin D. Haggerty, "[r]isk society operates within a negative logic that focuses on fears and the social distribution of 'bads'. Collective fear and foreboding underpin the value system of the unsafe society, perpetuate insecurity, and feed demands for more knowledge of risk."[1180] This demand for more knowledge of risk in turn feeds the craving for more information collection. For the state as protector, such information collection appears vital in an effort to establish *collective* security. Whereas the overview in section 3.4 proved more reflective on the instruments implemented to accomplish *individual* security, the competition between both hovered in the background. The objective of collective security considers privacy its enemy rather than its friend. This juxtaposition is problematic for privacy, or more specifically data protection, is an instrument of *individual* security. This dichotomy is masterfully subjected to scrutiny by the Committee Brouwer-Korf in the Netherlands. This scrutiny exposes the potential flaws of reasoning in the portrayal of a dichotomy between privacy and security, for information collection and storage can also lead to a potential state of *insecurity*.

The events of September 11, 2001 and the overall fight against terrorism increased the desire of the state to accumulate more information. The passage of the USA Patriot Act of 2001 provides a prime example of this cause and effect development. Priscilla M. Regan provides a detailed overview of the expansion of powers granted to the state through the implementation of the USA Patriot Act.[1181] Based on her overview she states, "[a]lthough an omnibus approach to privacy protection has traditionally been viewed as inappropriate in the United States, an omnibus approach to privacy reduction in the face of terrorism appears now to be appropriate."[1182] Collective security then trumps individual security.

This thrust for more information collection also proved its presence in the European Union. In a framework decision proposal, the Council of the European Union writes "[s]ince 9/11, law enforcement authorities around the world have come to realise the added value of collecting and analysing so-called PNR data in combating terrorism and organized crime."[1183] The Council furthermore notes

---

[1178] For a more extensive description of how information embodies these attributes see Newman & Clarke (2003): 70 – 77.

[1179] Ericson, R. V. & K. D. Haggerty (1997). *Policing the risk society*. Toronto: University of Toronto Press.

[1180] *Ibid:* 449.

[1181] Regan, P. M. (2004). Old issues, new context: Privacy, information collection, and homeland security. *Government Information Quarterly*, Vol. 21: 481–497.

[1182] *Ibid:* 483.

[1183] Council of the European Union (2007). Proposal for a council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes: 2.

how "[t]he collection and analysis of PNR data allows the law enforcement authorities to identify high risk persons and to take appropriate measures."[1184] This demonstrates the continued connection made between risk reduction and the accumulation of information. Besides PNR data, the United States also desires information on bank account related matters from the European Union. According to the United States government, access to such data is vital for the efforts to prevent terrorist financing. Vice-President Biden specifically stated how "[t]he longer we are without an agreement on the terrorist-finance tracking programme, the greater the risk of a terrorist attack that could have been prevented."[1185] Once again, risk prevention dominates the demands.

The usage of 9/11 as a justification for this information collection is surprising especially since the 9/11 Commission makes no mention of a lack of information. Instead, the Commission focused much of its attention on problems associated with information sharing. "We learned…" the Commission states, "…of the pervasive problems of managing and sharing information across a large and unwieldy government that had been built in a different era to confront different dangers."[1186] The focus is on managing and sharing information, not on its collection. In fact, the Commission details the considerable collection of reports on the possible threat of a terrorist attack. More specifically, the Commission writes how "[i]n the spring of 2001, the level of reporting on terrorist threats and planned attacks increased dramatically to its highest level since the millennium alert."[1187] By the time the Summer of 2001 arrived, the 'system was blinking red.' Despite the blinking, "…no one looked at the bigger picture; no analytic work foresaw the lightning that could connect the thundercloud to the ground."[1188] The lack of connection between individual cases failed to develop the threat into a national priority. As noted in section 3.2.1, during the background sketch of the FBI and its reprioritization process, the events of September 11 found themselves cast as the result of an intelligence failure. The call for more information inherently contradicts the conclusions of the Commission on the lead up to the events. Moynihan & Roberts describe the significant light September 11 shed on the problems of coordination within the United States government. They write how, "[t]he September 11 attacks highlighted failures in coordination within the intelligence community, between intelligence agencies and federal law enforcement agencies, and between the four agencies—INS, Customs Service, Coast Guard, and Bureau of Consular Affairs—responsible for border management."[1189] Problems of coordination originated through technical as well as organizational channels, where obstructions to collaboration often occurred due to poorly integrated or incompatible information systems. The Commission itself wrote how "[t]he agencies are like a set of specialists in a hospital, each ordering tests, looking

---

[1184] *Ibid.*

[1185] Biden calls on EU help to face 21st Century threats (2010). Available at: http://www.euractiv.com/en/priorities/biden-calls-on-eu-help-to-face-21st-century-threats-news-493858

[1186] National Commission on Terrorist Attacks upon the United States (2004). *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*: xvi.

[1187] *Ibid:* 255.

[1188] *Ibid:* 277.

[1189] Moynihan, D. & A. Roberts (2002). 'Public Service Reform and the New Security Agenda,' in *Governance & Public Security*. Washington, DC: Campbell Public Affairs Institute: 140.

for symptoms, and prescribing medications. What is missing is the attending physician who makes sure they work as a team."[1190]

The Netherlands proves to be hardly any different. The advisory committee on data flow security reached similar conclusions to the 9/11 Commission.[1191] The advisory committee aimed to analyze the systemic approach used by those involved in national security with respect to information collection from external databases. Such a systemic approach did not exist.[1192] Instead the advisory committee discovered how all agencies used different approaches to carry out their information collection activities. Those involved in the area of security lack a common vision on the importance of external databases for the development of information and intelligence.[1193] Closely related is the lack of cooperation between the various parties involved within the security realm. Despite the expansive growth of the number of databases and the importance of such databases for security, their existence and usage receives insufficient political and administrative attention. Simultaneously, strategic attention with respect to the information maintained in these databases is also absent. The actual collection of information is fragmented and realized through a sectoral approach.[1194]

Charles den Tex reflects on the information collection practices of the State and describes how Corien Prins previously noted that "[t]he government's approach to cyber crime is insufficient, and what is more, the government actually stimulates cyber crime by not trying to curb its own information hunger and that of companies."[1195] Den Tex in turn responds and cleverly states: don't you just love the way she calls it information HUNGER. That's neat, isn't it. HUNGER. By saying it is HUNGER, she is saying that is really a natural drive. You can't fight hunger, you have to eat. It's natural. Governments, companies and especially large companies, all over the world have this insatiable HUNGER. The poor things. It is not Hunger, of course, it is obsession. Pure obsession. What they need is therapy. Intensive therapy. Their information hunger has turned into to full scale irreversible information obesity. They cannot live without feeding their obsession."[1196]

The obsession expressed by governments is exacerbated by the developments in the corporate world. The proliferation of information brokers, especially in the United States, demonstrates the profitable nature of catering to the information obsession of both the public and the private sector. This availability and accessibility in the data brokerage industry also managed to attract the attention of perpetrators of financial identity theft. ChoicePoint remains the embodiment of this aspect of the opportunity structure. Its existence and its practices nevertheless cater to the quest for collective security and as such trump the threat the broker poses to individual security. Robert O'Harrow highlights the beneficial impact of the events of September 11 on the business of ChoicePoint. For "[s]uddenly everyone was uneasy, and not just about terrorists."[1197] Data brokers manage to fill a void through providing law enforcement with more information than can be

---

[1190] National Commission on Terrorist Attacks upon the United States (2004): 353.
[1191] Adviescommissie Informatiestromen Veiligheid (2007). *Data voor daadkracht. Gegevensbestanden voor veiligheid: observaties en analyse.*
[1192] *Ibid.*
[1193] *Ibid.*
[1194] *Ibid.*
[1195] Qtd. In den Tex, C. (2010). Speech presented on SuperTU/Esday, Eindhoven, February 11, 2010.
[1196] *Ibid.*
[1197] O'Harrow, R. (2006). *No Place to Hide.* New York, NY: Free Press: 154.

legally obtained via public sector channels. As a result, the usage of information brokers by the state, in particular law enforcement, nurtures the existence and subsequent survival of the industry.[1198] This reliance functions as a facilitation of the first stage of financial identity theft. For as the data security breach of ChoicePoint demonstrated, perpetrators of financial identity theft target the industry for the acquisition of personal information. This is especially due to abundance and availability of such information. The reliance of the state itself on the existence of the industry also leads to a conflict of interest for the existence and the practices of the industry threaten individual security, but the state uses its services in an attempt to establish collective security.

The information brokerage industry in the United States maintains a more expansive character than in the Netherlands. As section 7.1.2 indicated, the information brokerage industry in the Netherlands is hardly an industry of a similar nature for such information agencies cater to a smaller population and actually are more carefully scrutinized by the Data Protection Authority office. The 'industry' remains restricted to the needs of debt collectors, attorneys, and others. And as such, it seems as though perpetrators of financial identity theft have not identified these information agencies as a suitable target for their activities.

Even so, the abundance and availability of information are not in and of themselves the most problematic aspects with respect to the facilitation of financial identity theft. The accessibility of such information by perpetrators of financial identity theft is. Lawrence E. Cohen & Marcus Felson included access as one of the four elements derived from human ecology to determine the suitability of targets (see section 1.2), which underscores the importance of accessibility within an overall opportunity structure for financial identity theft. Accessibility of information increased as a result of advances in digital technology. Such accessibility proved a welcomed addition for the state as provider, but also introduced a conflict with its role as protector. The digital accessibility of the information maintained by the state both as protector and as provider in turn hypothetically opens the door to increased intrusion by perpetrators of financial identity theft. The developments in the Netherlands with respect to the Municipal Personal Records Database offer many benefits in terms of efficiency and convenience; yet, the GBA-V which provides for online access to a central version of the database requires sufficient security to prevent access by those interested in the acquisition of personal information in an effort to carry out acts of financial identity theft. The background of the developments surrounding the GBA-V, however, demonstrates the focus on efficiency and convenience, along with a need for modernization of the system (see section 4.1.1).

To frame the changes in a sense of modernization also allows the transformation to carry an air of progress which is a more general trend in contemporary society with respect to technological developments. The complexity of interests associated with technological innovation and societal 'progress' is powerfully captured by Ullrich Beck. He writes how "...the demonstration of side effects (at least at an early date) collides with the economic and economic policy interests that are invested in the chosen path of technological development. The

---

[1198] See *Ibid*; Hoofnagle, C. J. (2004). Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement. *North Carolina Journal of International Law and Commercial Regulation*.

more the side effects (or public sensitivities to them) grow and the greater the interest in economic recovery becomes (also in view of mass unemployment), that much narrower becomes the freedom of action for technology policy, which is caught between the milestones of a critical public and economic priorities."[1199] To resolve the conflict of interest, or to relief the conflict, those in favor of technological innovation frame their investments through the idea of progress. Beck succinctly captures the essence of the model of progress when he writes, "[p]rogress is a blank page as a political program, to which wholesale agreement is demanded, as if it were the earthy road to heaven."[1200] The promise of progress silences the cries of the critics. The technological promise of efficiency appeals to those in the public and the private sector, whereas its convenience attracts the permission of the public (see section 8.1.4). This is problematic since the challenge of security remains, which finally found itself in the spotlight as a result of the media reports on data security breaches. As became evident in section 3.4, such stories led to sufficient political pressure to invite the attention of policy makers. Simultaneously, the background also demonstrates the shortfall of instruments of data protection to fulfil their purpose with respect to individual security. Whereas data security breaches prove to be the representation of such a shortfall, its occurrence also characterizes the treatment of personal information in contemporary society, in both the United States and the Netherlands. The promise of progress enhanced through technological advancements often managed to overshadow the potential perils of such developments. This changed in part due to the involvement of the general public. For the United States, the Watergate scandal (see section 3.3.1) generated sufficient attention to accumulate political pressure, whereas in the Netherlands the census of 1971 accomplished a similar task (see section 3.3.2). Even so, other threats, especially terrorism, manage to generate significant momentum to allow the pendulum to swing the other way.

The private sector, including financial service providers, also engages in the information collection process. Richard J. Sullivan succinctly captures the problem when he writes, "[m]ore information will generally lead to a more accurate approval decision, which gives card issuers (and merchants) an incentive to continuously expand the data on which they rely. Criminals also have strong incentives to gather and use this same information to commit fraud. The incentives of these two groups results in an escalating cycle that leads to more resources on each side to either protect or to compromise data."[1201] This demonstrates the presence of double edge swords which plague many aspects of the opportunity structure of financial identity theft (see section 8.3.5).

The provision of information continues as a red thread of facilitation through all actors, including consumers. For consumers, the digital world is like a virtual playground. Social Networking Sites (SNS) provide the most illustrative example of the web 2.0 boom. The popularity of Facebook and Twitter continue to skyrocket. The appeal of SNS to share vast amounts of information also increases the public availability of such information. Much information is about mundane whereabouts and daily activities, but another share of the information is more personal and therefore more valuable. The eagerness of consumers to share personal information in the virtual world is magnified by the ability of third parties

---

[1199] Beck, U. (1992). *Risk Society: Towards a New Modernity*. London: SAGE: 213-214.
[1200] *Ibid*: 214.
[1201] Sullivan, R. J. (2010). The Changing Nature of U.S. Card Payment Fraud: Issues for Industry and Public Policy. *Workshop for the Economics of Information Security (WEIS)*: 3.

to gain access to such information (see section 6.2.1), since such information is a source of profit for SNS. Even so, important to note is how the membership of a SNS remains a choice rather than an obligation. The revolution surrounding the practices of SNS seems to at times forget this aspect of the debate, especially since SNS have managed to evolve into a near necessary element of life in contemporary society which raises the stakes for members of the sites.

For perpetrators, personal information is the key to the kingdom. The abundance and availability of personal information is important, but its accessibility is vital. This accessibility is mainly achieved via the digitalization of information, which is an integral aspect of contemporary society since such digitalization comes accompanied by the benefits of efficiency and convenience. This is especially so since such access to information is no longer bound by time or location which leads to a sense of 'progress.' This 'progress' is important in a society where speed is of the essence since instant gratification has become common place. Moreover, the focus on risk assessment and risk reduction, and the role of information played to achieve such objectives also enhances the importance of instant accessibility and as such requires the implementation of advanced means of digital technology. The necessity for improved security alongside this increased accessibility, however, remains underacknowledged or simply ignored.

8.1.2 'Function Creep'

Information acquires its value due to its purpose in contemporary society. The expansion of the purpose of information, especially in the virtual world, therefore logically leads to an increase in its value. The above section mainly referred to the aspect of the opportunity structure which caters to the first stage of financial identity theft, the information acquisition stage. This section instead shall cover how the overarching theme of function creep led to the potential and partial facilitation of the second stage of financial identity theft.

Several instruments introduced by governments experience an expansion of applicability or 'functions' beyond their original intent. This is often referred to as function creep, or its more negative alternatives 'surveillance creep' and 'control creep.'[1202] Whether such a function expansion is positive or negative is based on a value judgment,[1203] especially since such expansion can maintain both advantages and disadvantages. As Dahl and Saetnan write, "[t]he term function creep may in a given case refer to the skin-crawling, chilling nature of the latest added function and/or the sneakiness of an undemocratic, secretive process of socio-technical change…but it may also simply refer to slow, considered, and accepted change."[1204] Even so, this section analyzes the increased risk of financial identity theft as a result of function creep.

The most prominent example of function creep is the usage of Social Security Numbers in the United States. Former President Roosevelt introduced the Social Security Number with a specific purpose, but as became obvious in section 4.2.1 the original intent is lost in its expansion of uses across both the public and the private sector. This state of affairs is difficult to comprehend in light of its

---

[1202] Dahl, J. Y. & A. R. Saetnan (2009). "It all happened so slowly"–On controlling function creep in forensic DNA databases. *International Journal of Law, Crime and Justice*, Vol. 37: 83 – 103.
[1203] *Ibid.*
[1204] *Ibid:* 85.

historical background, since in the early days no proof of identification was required to obtain a social security card. Moreover, the main problem of the function creep of Social Security Numbers is the reliance on the instrument for verification purposes despite its public availability and accessibility. The problem for financial identity theft therefore is the value of the number which makes it an attractive object for perpetrators as an instrument to carry out acts of financial identity theft. This is a problem familiar to many in the United States and abroad, but remains a difficult challenge to respond to by the government. This is mainly the result of the advantages associated with the function expansion of Social Security Numbers. For such an expansion provided both the public and the private sector to benefit from an existing system which meant additional costs remained out of sight. In addition, the usage of the number is convenient for the public and the private sector as well as citizens and residents.

The developments with respect to identity numbers in the Netherlands demonstrate a vague resemblance to the early days in the United States when function creep began to occur. This resemblance is evident through the transformation demonstrated by the government from a historical perspective. Initially, as became evident in section 4.2.2, the government proved resilient against the evolution of the social-fiscal number into a general identity number. This resilience in theory failed to translate into practice as the social-fiscal number did become the de facto identity number. When the government introduced the citizen service number, it demonstrated an acceptance of the state of affairs at that time and made it official. The expansion of the citizen service number into the health care sector demonstrates its function creep into other sectors. The evidence to demonstrate the escalation of function creep also becomes evident through the proposal to provide for the usage of the number in the sector of financial services. In retrospect, it is interesting to note how during the parliamentary discussions on the topic of the introduction of a citizen service number, the government refrained from discussing its potential usage by institutions outside of the public sector. And as a result, the current developments with respect to the health care and financial services sector demonstrate how function creep occurs at a later stage and in a more incremental fashion. The comparison to the frog and the pot of boiling water is therefore a suitable metaphor. The incremental nature of the function creep with respect to the citizen service number manages to fragment the potential 'threat' which makes the danger of such a threat appear low. The early warnings[1205] issued against the function creep of the citizen service number therefore do not maintain a significant impact on developments in the public policy arena.

Due to the potential for future legal authorization, where additional usage of an instrument becomes part of the legal framework during a later stage, Pounder calls function creep an inevitability and therefore states how such function creep should be anticipated.[1206] As such, Pounder states how the focus should be on whether the legal framework in place provides sufficient means of protection when such function creep occurs. For the United States, the answer appears to be negative, since the framework proved ineffective as an instrument of protection

[1205] See Prins, J. E. J. (2003). Het BurgerServiceNummer en de strijd tegen Identiteitsfraude. *Computerrecht* (1): 2-3; Grijpink, J. H. A. M. (2006). Identiteitsfraude en overheid. *Justitiële Verkenningen*, Vol. 32 (7): 37 – 57.

[1206] Pounder, C. (2008). Nine Principles for Assessing Whether Privacy is Protected in a Surveillance Society. *Identity in the Information Society*, Vol. 1 (1).

for the people against problematic function creep. Furthermore, the situation in the United States also demonstrates the challenges introduced as a result of the need to restrict the negative consequences of function creep. To restrict the negative consequences, a reversal of function creep itself must occur, which often implies the introduction of a different system to allow the original system to return to a more specific purpose and to reduce its value and its attractive nature for perpetrators of crime. This is difficult because of the costs associated with the introduction of a different system and because the reversal of function creep is more challenging than the actual function creep itself. Metaphorically speaking, it is easier to pour the liquid out of a bottle into a glass than vice versa.

The existence of function creep in other areas of the identification infrastructure enhances its importance in the overall development of an opportunity structure for financial identity theft. The usage of 'identification' documents is another pertinent example. In the United States, the driver's license is the de facto means of identification used for identification purposes and accepted by the public and the private sector. This surpasses the original intent of the driver's license, which is to demonstrate someone's legal capacity to operate a vehicle. Once again, from a perspective of convenience and efficiency this is understandable; yet, such function creep increases the value of the document for perpetrators can use them as means of identification which surpasses the specific purpose of the license. In the Netherlands, the driver's license also carries multiple functions, just as the passport. The plan to incorporate a chip onto the driver's license which shall also evolve into an electronic identity demonstrates the intention to use an existing system and benefit from its potential to encompass multiple functions. Dahl and Saetnan summarize this underlying motivation of function creep when they write, "[o]nce a technology is in place, it becomes wasteful not to use it to the fullest acceptable limit."[1207]

Even so, there is a vital difference between the situation in the United States and the Netherlands. As a member state of the European Union, the Netherlands is subject to the decision making at the European level. As a result many developments which attempt to both enhance and harmonize identification documents in the European Union influence the quality of the document in the Netherlands. This transnational influence was a positive one several decades ago when the passport in the Netherlands carried a particularly negative reputation as a result of its sensitivity to fraud (see section 4.3.2). From a situational crime prevention perspective, the standardization requirements led to an increase in the effort which had to be made by perpetrators of identity theft to falsify the document. This, however, did lead to displacement of the problem to the issuance process, which the state has since responded to over the years. Overall, the situation in the Netherlands sketches a scene where the importance of identification documents, whether passports or driver's licenses, is reflected in efforts to ensure the integrity of both the quality of the product and the issuance process. Whereas originally both demonstrate vulnerabilities, the government has made changes to improve both the product and the process. This is important since such efforts aim to mitigate the potential negative impact of function creep, since these efforts complicate the attainment of the document or the falsification of such a document.

[1207] Dahl & Saetnan (2009): 89.

The United States, on the other hand, remains caught in a situation filled with tension and resentment. The REAL ID Act aimed to harmonize and enhance the quality of driver's licenses but found itself in the midst of various debates. From a perspective of Federalism, the involvement of the Federal government proved controversial for the issuance of driver's licenses is outside of its scope and falls under the sovereignty of the states. Other sentiments which focus on the connection between the potential abuse of power and the implementation of a national identity card also complicate the efforts made by the government in the United States. As a result, improvements with respect to both the quality of the document as well as the issuance process remain subject to variation based on the perspective of the different States.

The overarching 'instrumental' function creep can also be extended to the functionality of the computer which, in contemporary society, has significantly expanded and as a result also led to an expansion of opportunities. Much like the stretch of an elastic band, such an expansion of functionality increases the tension and places a higher pressure on the security of the instrument to prevent it from 'snapping.' This is where perpetrators of financial identity theft have managed to take advantage of the function creep, since their innovative methods of attack have generally surpassed the capacity, or the willingness, of both the public and the private sector to resist such attacks. This is problematic since the function creep is a continuous process, especially with respect to the delivery of 'services' by the state via the Internet, as well as private sector activities such as Internet banking.

The spread of applications for the mobile environment also demonstrates function creep which in turn expands opportunities and suitable targets. The mobile environment did not necessarily feature as an integral aspect of the opportunity structure throughout the previous chapters, but instead hovered in the background and ought to receive more attention in light of future applications. The usage of the mobile phone for transactions (see section 5.4.2) as well as for means of authentication (see section 4.4.2) demonstrates its function creep. This function creep is the result of both efficiency and convenience (see section 8.1.2). Jon Giffin notes how "[m]alware commonly targets personal desktop systems, and the rapid changes happening today in personal computing offer new opportunities for attackers. Infections are poised to spread to mobile environments. The recent emergence of smart phones as viable, full-featured systems provides an entirely new collection of attack targets."[1208]

Overall, the most fundamental problem with function creep is the development of a single point of vulnerability, which when compromised subsequently paves the way for the facilitation of financial identity theft. The existence or potential for function creep within the identification infrastructure developed by the state as provider is widespread. This is in large part due to the efficiency of function creep and its accompanying convenience.

8.1.3 From Elite to Mass

Certain features covered in the previous chapters demonstrate a historical progression from an instrument available exclusively to an elitist crowd into an instrument of the masses. This transformation is important on two different

[1208] Giffin, J. (2010). The Next Malware Battleground. *IEEE Security & Privacy*, Vol. 8 (3): 74.

dimensions. First, such a transformation changes the scale of the feature and therefore increases the applicable population. This increase also translates into an increase of suitable targets for perpetrators of crime, as the routine activity approach recognizes as a crucial element (see section 1.2). The difference between MAC and PC users demonstrates this difference of scalability. To this day, the majority of end users are PC users which makes the PC, or its users, more suitable as a target. This is in contrast to the smaller MAC population. The increase of suitable targets for financial identity theft occurred, in part, through the transformation of credit cards from an instrument associated with the elite to a tool used by the masses to purchase goods on credit. The same goes for the transformation of the passport from a privilege to an obligation (see section 4.3).

Second, a transformation from elite to mass means the population which can gain access or entry to a particular tool or feature also increases, which often means the entry requirements decrease which changes the overall access control. This change in entry requirements is an important aspect of the opportunity structure since perpetrators of financial identity theft manage to take advantage of this lowered threshold. Credit cards demonstrated their historical progression from an elitist product into a means for the masses to purchase goods and services on credit. Such a progression increased the interest of financial service providers to attract as many clients as possible. This became evident through the marketing practices of the mass distribution of unsolicited credit cards (see section 5.1.1). Whereas the United States government stepped in to curb these practices, other marketing instruments such as the mass distribution of pre-approved credit card applications still provide opportunities for perpetrators of financial identity theft. And besides the marketing instruments, the application process involved in the credit card procedure also demonstrates the decrease in requirements as a result of the endemic dilemma, where lower entry requirements lead to more applicants and profit but also to more fraud (see section 5.2.1). The absence of such practices in the Netherlands along with the absence of mass appeal for credit cards to the Dutch population provides for a more limited opportunity structure in this regard. The credit card in the Netherlands maintained an exclusive character, only to be used when other alternatives proved unavailable (see section 5.1.2). This is hardly the case in the United States which is the epitome of a 'credit card nation.' Robert D. Manning writes how "[a]fter celebrating the arrival of the new millennium, American society registered another less publicized millennial milestone: almost 1.5 billion consumer credit cards. That's right, *1.5 billion cards* held by nearly 158 million cardholders. That's an average of ten credit cards per cardholder."[1209] According to Manning, consumer credit has become the lifeblood of the economy in the United States since the early 1980s. As a matter of fact, Manning describes how credit cards play such a prominent role "…in influencing domestic economic trends (inflation, GDP, and employment) that President Carter in 1980 and President Bush in 1991 sought to regulate officially the availability and cost."[1210] This demonstrates the character of necessity of credit cards in the United States and also provides a context for the continuous promotion of the product.

Another development which resembles a similar historical progression and subsequently evolved into an opportunity for perpetrators of financial identity

[1209] Manning, R. D. (2000). *Credit Card Nation: the Consequences of America's Addiction to Credit*. Basic Books: 5 – 6.
[1210] *Ibid:* 6.

theft to profit from is the background of Facebook. As section 6.2.1 demonstrated, perpetrators of financial identity theft target SNS, especially Facebook, to acquire personal information or to transmit malicious software. Whereas Facebook currently maintains massive appeal and users from all over the world, its historical roots demonstrate its elitist nature. Originally, Facebook was only available and accessible for individuals, whether students or employees, from a select group of universities in the United States. Facebook carried out access control through only allowing individuals in the possession of an email address from member universities to establish a profile. This meant the right to access Facebook was viewed as a privilege. This observation is reinforced through my personal experience since Facebook provided the University of Maryland, Baltimore County access to its site in 2005. This became headline news for the university as the student newspaper covered most of its front page with a story about this 'privilege.' Much has changed since then, especially since Facebook is no longer a privilege. Some might even argue how in contemporary society Facebook is a necessity much the same as a passport or a credit card. The most crucial aspect of the transformation engaged in by Facebook is the elimination of access control which translates into facilitation for perpetrators of financial identity theft to gain access to the site and to the personal information posted on the profiles. Certainly Facebook introduced privacy options which allowed users to guard their profiles, but as Bilge *et al.* demonstrated through profile cloning, perpetrators still maneuver their way to the personal information maintained in a profile.[1211]

The transformation from elite to mass overall demonstrates an increase in a population of suitable targets as well as a reduction in access control which negates an opportunity reduction technique as identified by the situational crime prevention framework. Through such a decrease in access control, perpetrators take advantage of the ability to obtain access to valuable targets such as personal information and credit cards.

8.1.4 The Cost (and Profit) of Convenience

Many of the facilitating factors which surfaced throughout the previous chapters, especially chapter 4 and 5, illustrate the connection between convenience and the facilitation of financial identity theft. As a result, the facilitation of financial identity theft is the cost of convenience. This can be observed through several facilitating factors. Among the most prominent factors are the acquisition and application process used for financial services in the United States. The distribution of unsolicited credit cards as a marketing instrument aimed to appeal to the convenience craving of consumers. As the Board of Governors of the Federal Reserve System notes, "[f]or consumers, prescreened solicitations reduce search costs by providing them with ready information about product availability and pricing tailored more closely to their financial experiences and needs. Such screening also increases the likelihood that consumers responding to such solicitations qualify for the product or service being offered and thereby reduces the possibility that the consumer will be wasting his or her time and effort when

[1211] Bilge, L., Strufe, T. Balzarotti, D. & E. Kirda (2009). All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks. Paper presented at the *18th International World Wide Web Conference*.

responding to a mailing."[1212] Simultaneously, the convenience of the application process is intended to maintain a smooth path for consumers to apply for a credit card or another financial service.

Such convenience again returns during the account activity of Internet banking in the United States. Despite the awareness about the security implications of a single factor authentication scheme, such scheme offered the much desired convenience which is viewed as a necessity to keep consumers content. As a result, while the facilitation of financial identity theft is the cost of convenience, the profit rests in the ability of such convenience to maintain and attract clients.

This focus on convenience in the financial services industry is less dominant in the Netherlands, where the sector itself is the object of more strict regulation but where the more limited number of players in the field also provides for a more balanced approach to security and convenience. This is apparent through the lack of aggressive marketing practices by the industry with respect to the acquisition process of prospective clients. The application process, especially the historical development, demonstrates how whereas several decades ago problems surfaced with respect to the identification of clients and the facilitation of fiscal fraud this changed through the introduction of a code of conduct (see section 5.2.2). The developments at the international and subsequent European level led to more changes and to a greater involvement of the state. The focus as a result remained more on security than on convenience. The same in turn applies to the introduction of Internet banking activities where security proved an integral aspect of the architectural development of such activities (see section 5.4.2). The Dutch Central Bank also played an important role as supervisory organ to ensure the aspect of security received sufficient attention by the financial service providers. While the absence of prevalence data only provides for hypothetical conclusions, this difference in approach with respect to the aspect of security and convenience in both the United States and the Netherlands appears to maintain a significant impact in the potential for facilitation of financial identity theft. This difference seems to be the result of scalability which in turn influences competition and priorities. The limited number of providers in the Netherlands appears to stimulate the development of an understanding, avoid free riders, and as such paves the way for a more appropriate balance between convenience and security.

The interdependency of the problem is more pronounced with respect to convenience in the financial services industry in the United States than in the Netherlands. The lack of solidarity as a result of the fierce competition also makes financial service providers less inclined to improve their means of security since in so doing they may increase the threshold and lose clients to competitors.

For merchants, on the other hand, convenience plays a role in the adoption of improved means of security in the Netherlands. For the introduction of an additional hurdle through the 3D Secure system led many to demonstrate a hesitant stance due to the fear of losing clients to another online store (see section 7.3). This is precisely why the introduction of an instrument of security requires solidarity among those within the industry, since such solidarity minimizes the potential for loss of clients and as such convenience loses its power as an argument against security.

[1212] Board of Governors of the Federal Reserve System (2004). *Report to the Congress on Further Restrictions* on Unsolicited Written Offers of Credit and Insurance: 3.

The contested relationship between convenience and security returns with respect to the government as provider, and in particular the introduction of e-government applications. The transformation of citizens into consumers led to a focus on service delivery. This became evident in section 4.4 as did the potential implications for the connection between convenience and security. Both the United States and the Netherlands recognized the need for the existence of multiple levels of identity authentication depending on the service and the transaction offered via the Internet. Even so, the introduction of DigiD as a means of electronic authentication in the Netherlands based its single factor authentication system more on convenience than on security (see section 4.4.2). For usability proved an important feature for the government in the Netherlands, since the government wanted to attract citizens to use the electronic superhighway in an effort to reduce the administrative burdens of various operations, especially tax returns. DigiD in the Netherlands is convenient and represents the lowest level of security. This changed through the addition of a text message as another aspect used for the authentication of the citizen. And the plans to revamp the system, DigiDX, also demonstrate awareness about the need to adjust the system according to the potential proliferation of more electronic services.

The importance of convenience as an aspect of the opportunity structure is evident through the suggested countermeasures. Certain off hand pieces of advice already demonstrate the need to backtrack on convenience as a means to improve security and achieve a sense of situational crime prevention. During his inaugural address, Sandro Etalle notes how "[t]o start with we can use one computer to visit untrusted sites and download untrusted software from the internet, and another computer to do business and internet banking."[1213] This might certainly help matters; yet, such a suggestion refutes the primary appeal of Internet banking, which is its lack of attachment to a particular time or location. So the suggestion put forth by Etalle is valuable but its value rests in the willingness to trade convenience for security, which emphasizes the overall cost of convenience as a means of facilitation of financial identity theft.

8.2 Countermeasures

The second part of this chapter aims to shed light on the existing countermeasures and to assess them in light of the above opportunity structure as well as according to the opportunity reduction techniques as set forth by the situational crime prevention framework. Important to (briefly) reflect upon before discussing existing countermeasures is the tension between economics and security. As the previous chapters along with the above described opportunity structure demonstrate, the facilitation of financial identity theft must be observed within its proper (social) context. This context includes the underlying mechanisms which nurture the facilitating factors and also illustrate how much facilitation occurs as a result of a cost benefit analysis. This same economic perspective returns with respect to countermeasures, where the investment of the security measure must arguably outweigh its costs in order to be worth the effort. The importance of the economical perspective returns in the literature and demonstrates how the effective countermeasure share a commonality, which is the ability to influence the

[1213] Etalle, S. (2008). *Nice to know*. Inaugural lecture Eindhoven University of Technology, October 3, 2008.

(economical) incentives of the targeted actor. All four aspects of the opportunity structure demonstrate how much of the decision making process to implement particular features is based on the ability to work in a more efficient manner and as a result generate more profit or in the case of the state lower the costs, which especially during the most recent financial crisis, is particularly lucrative. The criticism addressed against existing countermeasures must therefore bear in mind that viable alternatives are scarce, at least alternatives which manage to provide an acceptable cost-benefit balance.

To provide a structure for the analysis of existing countermeasures, the situational crime prevention framework as briefly discussed in section 1.2 shall be used. This framework identifies four different categories of crime reduction techniques which each carry four specific types of aims. This overview shall only focus on the first two categories introduced, since these capture most of the countermeasures discussed.

8.2.1 Increasing the effort

The major focus of countermeasures introduced against financial identity theft appears to focus on increasing the effort. The umbrella category of increasing the effort contains four different types of measures which include target hardening, access control, deflecting offenders, and controlling facilitators. According to Newman & Clarke, the first two types of measures are applicable to the e-commerce environment whereas the latter two appear less applicable.[1214] As a result, Newman & Clarke offer two alternatives which are more appropriate for the e-commerce environment. These two alternatives are safeguarding data integrity and authenticating identity.[1215]

The first technique, target hardening, refers to measures introduced to increase the effort of obtaining the target. With respect to financial identity theft, the main target is the money. Yet, the focus from a situational crime prevention perspective must also be on the tools or instruments used to arrive at the money. The main target therefore is information in the virtual world and instruments, whether identification documents or credit cards, in the physical world. The opportunity structure described above reflected on the importance of the accessibility of such information and other instruments for the facilitation of financial identity theft.

Both the United States and the Netherlands have introduced countermeasures which relate to target hardening. For information, both countries have engaged in public awareness campaigns in an effort to educate citizens about the potential misuse of information and as such the need for them to be cautious about providing personal information to third parties. The notion of consumer education as a means to raise awareness is evident in various sectors of society[1216] as is empirical research on their effectiveness, or lack thereof.[1217] While certainly

---

[1214] Newman & Clarke (2003): 112.
[1215] *Ibid.*
[1216] See for example Bruhn, C.M. (1997). Consumer Concerns: Motivating to Action. *Emerging Infectious Diseases*, Vol. 3 (4): 511 – 515; Wood, A.L. & O.F. Wahl (2006). Evaluating the Effectiveness of a Consumer-Provided Mental Health Recovery Education Presentation. *Psychiatric Rehabilitation Journal*, Vol. 30 (1): 46 – 53.
[1217] Brown, K., Mcllveen, H. & C. Strugnell (2000). Nutritional awareness and food preferences of young consumers. *Nutrition & Food Science*, Vol. 30 (5): 230-235.

consumer education is important in an overall action plan to counter financial identity theft, their role and value should not be overestimated.

Public awareness campaigns emphasize the need for anti-virus software and firewalls in an attempt to increase the effort of perpetrators of financial identity theft. Newman & Clarke also identify firewalls as an instrument of target hardening.[1218] Particular problems exist with the advice provided through consumer education efforts with respect to financial identity theft. The main emphasis on the installation of anti-virus software and anti-malware is problematic for various reasons. First, the effectiveness of anti-virus software is limited due the ability of perpetrators to circumvent such means of software protection.[1219] To circumvent detection perpetrators use rootkits. As Francis M. David *et al.* describe "[i]n order to surreptitiously control a compromised computer, an intruder typically installs software that tries to conceal malicious code. This software is commonly referred to as a rootkit. A rootkit hides itself and some malicious payload from the operating system, users and intrusion detection tools."[1220] Other options include releasing the malware at such a high speed that it can be installed before anti-virus software has the ability to be updated and offer consumers the necessary protection.[1221] On the positive side, certain security professionals claim security software is making significant progress and is becoming more pro-active in the detection of new malware threats.[1222] Even so, Stan Hegt notes how "...the importance of front-end software security solutions is stressed unnecessarily in current anti-phishing strategies because of the failure of current two-factor and two-channel authentication schemes."[1223] This statement supports the argument made in chapter 6 about the decreasing visibility and as such the decreasing ability of consumers to defend themselves against attacks from perpetrators of financial identity theft.

Second, the emphasis on anti-virus software also brings along other negative consequences. Rather than a means to combat cybercrime, public awareness campaigns and especially the emphasis on anti-virus software actually might serve to nurture other types of online fraud. The introduction of rogueware demonstrates the adaptability of cybercriminals and presents society, especially consumers, with yet another considerable challenge. Correll & Corrons define rogueware as "...any kind of fake software solution that attempts to steal money from PC users by luring them into paying to remove nonexistent threats."[1224] This fake anti-virus software looks remarkably professional. GOVCERT, the Dutch government computer emergency response team, remarks how the team noted an explosive growth in fake anti-virus software.[1225] Complaints about the existence of fake anti-virus software date back to at least 2000. Such fake anti-virus software

---

[1218] Clarke & Newman (2003).

[1219] See Fredrikson, M., Martignoni, L., Stinson, E. & S. J. J. Mitchell (2008). 'A layered architecture for detecting malicious behaviors.' *11th International Symposium on Recent Advances in Intrusion Detection (RAID 2008)*.

[1220] David, F. M., Chan, E. M., Carlyle, J. C. & R. H. Campbell (2008). Cloaker: Hardware Supported Rootkit Concealment. *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA: 296.

[1221] Ollmann, G. (2008). The evolution of commercial malware development kits and colour-by-numbers custom malware. *Computer Fraud & Security*, Vol. 28: 4 – 7.

[1222] Gold, S. (2009). A Newsworthy year. *Infosecurity*, Vol. 6: 24 – 28.

[1223] Hegt, S. (2008). *Analysis of Current and Future Phishing Attacks on Internet Banking Services*. Master Thesis Technical University Eindhoven: 95.

[1224] Correll, S-P. & L. Corrons (2009). *The Business of Rogueware: Analysis of the New Style of Online Fraud*. Panda Security: 3.

[1225] GOVCERT (2009). *Trendrapport 2009*. Digital version available at: http://www.govcert.nl

exploits the fear of users and their security conscience, according to GOVCERT.[1226] The increased fear generated among the public through consumer education efforts and the marketing of anti-virus software provides consumers with a gentle push into the hands of the criminals. Perhaps soon awareness campaigns will also commence to discuss the recognition of rogueware to make a complicated affair even more complex.

Other measures introduced to accomplish target hardening are data security breach notification requirements since these aim to increase the incentives for organizations to improve information security practices. The focus on incentives is important since as Ross Anderson and Tyler Moore note "…people have realized that security failure is caused at least as often by bad incentives as by bad design. Systems are particularly prone to failure when the person guarding them is not the person who suffers when they fail."[1227] This is precisely why Anderson noted several years ago in 2001 how the solution to information insecurity rests in regulation rather than technology.[1228] Data security breach notification embraces this regulatory need in an effort to establish improved information security which in turn ought to make it more difficult for perpetrators of financial identity theft to obtain information, or rather the target.

Whether such a mechanism is effective is difficult to presently assess, especially since the actual implementation of data security breach legislation is still in a state of infancy. Moreover, the effectiveness depends more on the specifics of the plan rather than the premise itself. From a hypothetical perspective, the incentive to produce improved information security focuses on a specific facilitating factor of information accessibility through information insecurity. As a result, the successful implementation of a data security breach notification framework can result in an opportunity reduction, at least for the first stage of financial identity theft. For such an effect to occur, however, the incentive must be there, which is dependent on the (potential) damage the organization shall experience after a breach. This is precisely because of what Anderson and Moore refer to when they write about the discrepancy between the guardian of the personal information and the party who suffers from the information insecurity.[1229] Potential intervening factors include desensitization which can occur when citizens receive an overload of notifications and as such shall not actually respond to the issue. Such a lack of response then fails to provide the incentive for organizations to improve their information security, since the potential loss of clients and as such profits is eliminated as a result of desensitization.

Research about the impact of data security breach legislation is limited, but available. Based on event study methodology, Kevin M. Gatzlaff & Kathleen A. McCullough conclude how they found "…evidence that the stock market responds negatively to announcements of breaches of customer and/or employee data at publicly."[1230] This negative reaction is enhanced when the affected firm refuses to provide details about the breach. Gatzlaff & McCullough furthermore

---

[1226] *Ibid.*

[1227] Anderson, R. & T. Moore (2006). The Economics of Information Security. *Science*, Vol. 314 (5799): 610.

[1228] Anderson, R. (2001). Why Information Security is Hard - An Economic Perspective. *Proceedings of the 17th Annual Computer Security Applications Conference:* 358-366.

[1229] Anderson & Moore (2006).

[1230] Gatzlaff, K. M. & K. A. McCullough (2010). The Effect of Data Breaches on Shareholder Wealth. *Risk Management and Insurance Review*, Vol. 13 (1): 77 – 78.

note how the negative reaction proved strongest during the most recent time period included in the study. This, according to the authors, might be due to the anticipated increase in the perceived costs as a result of legislative initiatives.[1231]

In addition to the aforementioned measures, both the American and the Dutch government also aimed to introduce measures to increase the effort of attaining identification documents. For the United States, the introduction of the REAL ID Act of 2005 aimed to function as a vehicle to complicate criminal and terrorist operations through the introduction of specific regulations about the requirements for the issuance process of driver's licenses by individual states. The REAL ID Act also covered aspects which concerned the quality of the document and as such aimed to enhance the resistance of the document against potential falsification. This demonstrates the dual approach necessary to improve the safeguards of identification documents against potential usage of these instruments for the successful completion of a financial identity theft operation. The Netherlands, plagued by its turbulent history of the passport, also introduced several measures to improve both the quality of the product and the process in an endeavor to increase the effort for potential perpetrators. Such an increase in effort appears relevant especially in light of the facilitating factor which transformed the passport from a privilege into an obligation which made the document more accessible and used for a wider range of purposes than in the past.

The effectiveness of the improvements made to the quality of the document, including the incorporation of additional technology such as biometrics remains a topic of discussion. Whether biometric technology could actually reduce the incidence of identity theft remains questionable, since such technology alters the *identification* rather than the *verification* process. Jan Grijpink & Corien Prins present the important distinction between these two different concepts. According to Grijpink & Prins, identification occurs when an individual establishes precisely who someone is. Verification, on the other hand, is the process where an individual establishes that a person is the same person as expected or basically that the person is who he or she claims to be.[1232] This distinction is important with regard to the introduction of biometric technology because, as Grijpink & Prins note, without stronger and more unpredictable verification biometrics will not be very effective. As the authors state, "[u]nfortunately, people are often unaware of the limitations of the customary forms of personal identification, so that verification is often placed on a par with identification. Even if a person can be compared on the spot with a photograph on an identity card, the one-off and isolated verification can never provide certainty that the person in question is actually who he says he is."[1233] Grijpink and Prins observe that, with the exception of criminal law enforcement, a personal identification along the lines of 'he is the same as…' is sufficient for the majority of legal transactions.[1234]

For the financial services sector, target hardening of information present on the magnetic stripe on the back of debit and credit cards is also an important aspect of the situational crime prevention framework. In the Netherlands, the

---

[1231] *Ibid.*

[1232] Grijpink, J. H. A. M. & J. E. J. Prins (2003). 'New Rules for Anonymous Electronic Transactions? An Exploration of the Private Law Implications of Digital Anonymity,' in C. Nicoll, J. E. J. Prins, M. J. M. van Dellen (eds.) *Digital Anonymity and the Law. Tensions and Dimensions*. Den Haag: TMC Asser Press: 249 – 269.

[1233] *Ibid:* 252.

[1234] *Ibid.*

introduction of EMV technology represents such target hardening in an effort to reduce the opportunities for account takeover (see section 5.4.2). Even so, Ben Adida *et al.* provide an overview of (potential) vulnerabilities in the EMV scheme and note "[w]e hope that this whistle-stop tour shows that whilst EMV is undeniably a robust and secure payment protocol at heart, there is so much matter and complexity around the edges to get wrong that there will be plenty to keep the criminals fed and watered in the future; we look forward in particular to phish and chips!"[1235]

For access control, the most well-known technique is the usage of pins and passwords; yet, as has become obvious due to the maturation of malicious software neither is able to offer much protection. As a result, the introduction of a two-factor authentication mechanism is important; the Netherlands has incorporated this aspect of access control. Even so, perpetrators of financial identity theft have demonstrated their capabilities of gaining access despite the existence of a two factor authentication system. The implementation of another means of authentication, the SMS message, then in turn again aims to restrict access control by potential perpetrators of financial identity theft. Despite the ability of perpetrators of financial identity theft to circumvent the system, however, it is important to maintain a balance in light of the tension previously identified between economics and security. Much more authentication elements inevitably eliminate the added value of online banking altogether, which is particularly undesirable in contemporary society.

The most important type of opportunity reduction technique identified by Newman & Clarke for financial identity theft is authenticating identity. Newman & Clarke actually advance the position advocating the exclusive acceptance of credit cards for merchants since "…opportunities for credit card fraud are rapidly decreasing…"[1236] This is difficult to assess, especially since credit card fraud, in particular account takeover type fraud, continues to remain a dominant category of financial identity theft. The industry has, however, made attempts to increase the effort and to enhance the means of authentication. This occurred originally through the introduction of the CVC codes, and later on through the 3D secure option. Both are vulnerable to circumvention, especially as a result of the proliferation of malware which can install keyloggers to obtain all information entered onto the screen.

The different measures taken to increase the effort all demonstrate how such attempts are often a means to stall for time. Especially for the financial services industry, the changes introduced are an illustration of the arms race which financial service providers, as well as retailers, are engaged in with perpetrators of financial identity theft. Another problem associated with the idea of increasing the effort is the specialization of the crime industry. The necessary tools, such as the various forms of malicious software as well as personal information, including credit card numbers, can be purchased on the Internet, which means the increase in effort shall only be effective if such an increase is strong enough to thwart the innovators of the attacks. Because when innovative attacks surface, the Internet provide access to anyone willing to pay for the instruments to carry out such

---

[1235] Adida, B., Bond, M., Clulow, J., Lin, A., Murdoch, S., Anderson, R. & R. Rivest (n.d.). Phish and Chips (Traditional and New Recipes for Attacking EMV). Available at: http://www.cl.cam.ac.uk/~rja14/Papers/Phish-and-Chips.pdf (last accessed July 14, 2010): 1 – 2.
[1236] Newman & Clarke (2003)*:* 121.

attacks which devalues the increase in effort intended to accomplish through the countermeasures.

A glance at the reduction of other crimes provides limited inspiration. Ben Vollaard provides empirical evidence for the success of government intervention in the Netherlands with respect to high-quality locks and burglary-proof windows.[1237] Starting in 1999, the government required all new-built homes to have these high-quality locks and burglary-proof windows. Through this government requirement, the Building Code needed to be adjusted accordingly. Vollaard describes how the change in the Building Code reduced the burglary risk in newly built homes by 50 percent. Through these results, Vollaard considers the government regulation for built-in security an effective means to lower crime and also determines how the regulation maintains considerable social benefits. The government regulation also proved more effective than other measures taken to lower levels of crime such as altering the preferences of potential offenders or the preferences of victims for precaution."[1238] Such built-in security may also be an attractive option for the threats described in this book. Egele *et al.* elaborate on such a solution when they "...propose to have defense mechanisms built into the browser itself to mitigate the threats that arise from drive-by download attacks."[1239] Such built-in security takes into consideration the limited ability of consumers to protect themselves against the most recent threats in the digital world. Perhaps the success of the physical world can be transported into the digital realm.

8.2.2 Increasing the risk

Increasing the perceived risk of a criminal act can occur through formal surveillance, surveillance by employees, natural surveillance, and exit/entry screening. For the e-commerce environment, Newman and Clarke note how this category of opportunity reduction techniques appears less relevant.[1240] And that the last technique of exit/entry screening is difficult to distinguish from access control in a digital environment. Even so, since the opportunity structure also takes into consideration various aspects of the physical world which facilitate financial identity theft this category appears quite relevant to review existing countermeasures.

The introduction of criminal legislation which specifically applies to perpetrators of identity theft in the United States provided a legal basis for dealing with the phenomenon as a crime. The main drive behind such legislation appeared to be the ability to recognize the victim and to provide a legal foundation for law enforcement to engage in identity theft investigations. The impact of criminalization therefore is more apparent in the periphery aspects of the problem rather than the actual ability to increase the perceived risk. This also became apparent through the research conducted into the views of convicted identity theft

---

[1237] Vollaard, B. (2009). Does regulation of built-in security reduce crime? Evidence from a regression discontinuity approach. *First Bonn/Paris Workshop on Law and Economics*, September 25-26.
[1238] *Ibid.*
[1239] Egele, M., Kruegel, C. & E. Kirda (2009b). Mitigating Drive-by Download Attacks: Challenges and Open Problems. Unpublished manuscript. Available at: https://www.iseclab.org/papers/inetsec09.pdf (last accessed July 14, 2010): 11.
[1240] Newman & Clarke (2003).

offenders.[1241] From a situational crime prevention perspective, criminalization is a limited means to function as crime prevention. This especially since the risk for perpetrators of financial identity theft is diminished by the ability of perpetrators to commit their crime at a safe distance through the Internet. This also leads to complications of enforcement as became evident in section 3.2.3.

Based on the opportunity structure, other measures which attempt to increase the risk include the changes made to the treatment of incidents of lost or stolen identification documents in the Netherlands (see section 4.3.2). The pilot study conducted in the municipality of Amsterdam proves to be the start of such changes which aim to increase the risk of individuals who file reports of lost identification documents. Through the involvement of law enforcement and the potential for an investigation, the risk of filing for a lost identification document in an effort to receive a duplicate increases. This countermeasure targets the high number of missing identification documents through an increase in surveillance during the response procedure of lost documents.

The government as protector also aims to increase the perceived risk in the financial services industry. This occurs primarily through a focus on the application process (see section 5.2.1). The United States Congress introduced the notion of 'red flags' through the Fair and Accurate Credit Transactions Act of 2003. These red flags are to serve as an instrument of surveillance by employees of financial service providers which is to lead to better detection of incidents of financial identity theft. This concerns the application process which, as became obvious, demonstrates its impact on the facilitation of financial identity theft through the emphasis placed on convenience and efficiency as opposed to security. Provisions from the USA Patriot Act also aimed to improve the identification procedures incorporated during the application process for financial services in the United States and as such increase the perceived risk of financial identity theft operations. The motive to introduce the requirement for identity theft prevention programs through the incorporation of red flags therefore takes into consideration a crucial aspect of the opportunity structure.

The effectiveness of the red flags approach rests in the simultaneous correlation between detection and action. This is because mere detection without the appropriate action or response makes the countermeasure ineffective as a means to reduce the facilitation of financial identity theft. Hoofnagle's analysis of fraudulent applications (see section 5.2.1) demonstrated how despite the presence of red flags, identified by an automated system, financial service providers still issued a line of credit. This makes the existence of red flags and its detection lack a contribution to the fight against financial identity theft.

Financial service providers also already use software to detect suspicious account activity (see section 5.4). This occurs both in the United States and the Netherlands and provides financial service providers with an opportunity to catch the act of financial identity theft before the transaction occurs. Through the use of such methods, perpetrators see the risk of their operations being unsuccessful increased.

The assessment made by Newman & Clarke about the lack of applicability of this category of opportunity reduction techniques within the virtual world appears accurate. The perception as well as the reality of risks on the Internet is low,

---

[1241] See Copes, H. & L. Vieraitis (2009). Understanding Identity Theft: Offenders' Accounts of Their Lives and Crimes. *Criminal Justice Review*, Vol. 34: 329 – 349.

especially in comparison to risks in the physical world. As a result, the increase in perceived risks as a deterrent to prevent financial identity theft can only serve as a supplement in a more comprehensive approach to the problem.

8.3 Challenges

As the above demonstrates, countermeasures introduced against financial identity theft are hardly a silver bullet, and understandably so due to the tension between economics and security. Moreover, existing countermeasures must also be observed in connection to the challenges associated with the general introduction of crime prevention or rather crime reduction policy. The introduction of countermeasures in the fight against financial identity theft encounters several challenges. Certain challenges are particular to the complex character of financial identity theft whereas others are more general challenges faced by the public policy arena. Besides the challenges associated with the introduction of countermeasures, the effect of existing countermeasures also encounters obstacles. The list presented below is not meant to be exhaustive or comprehensive. Instead, the aspects selected are intended to provide a general indication of challenges which must be borne in mind when suggestions for other potential countermeasures are considered.

8.3.1 Agenda Setting

In *Agendas, Alternatives, and Public Policies*, John W. Kingdon asks "[w]hat makes people in and around government attend, at any given time, to some subjects and not to others?"[1242] This question, which Kingdon goes on to answer in the remainder of his book, is vital to consider in an effort to develop an understanding of the response offered by the state to (financial) identity theft. Kingdon refers to the importance and relevance of indicators, focusing events, crises, and symbols. Especially indicators of a problem are crucial to its transformation into an issue of public policy worthy of political attention. Kingdon notes how there is a need for indicators of a quantitative nature. As one of his interviewees stated, "[i]t helps for a problem to be countable."[1243] The quest for prevalence data in both the United States and the Netherlands immaculately demonstrates this need for quantitative indicators. But as described in chapter 1 and 2, identity theft is hardly a 'countable problem.' Still, the determination to accumulate quantitative means on the problem continues and the numbers which surface function as a crucial impetus to attract the attention of the public policy arena, especially the statistics which originate in the United States.

The challenge of 'counting' incidents of identity theft also indicates the need for other aspects to push the item higher on the political agenda. Kingdon notes how indicators are in and of themselves insufficient at times and need the assistance of focusing events, such as a crisis or a disaster, a powerful symbol, or a personal experience of a policy maker.[1244] The rise of identity theft as a topic worthy of political attention demonstrates the essence of these aspects. Certain focusing events, such as September 11, 2001, placed vulnerabilities in the

[1242] Kingdon, J. W. (2003). *Agendas, Alternatives, and Public Policies*. New York: Longman: 1.
[1243] Qtd. In *Ibid*: 93.
[1244] *Ibid*: 94-95.

identification infrastructure in the spotlight and led to the passage of the USA Patriot Act of 2001 and the REAL ID Act of 2005. Despite the onset of identity theft during the previous years, September 11, 2001 put the issue of identification genuinely on the map. This connection between terrorism and the increased attention devoted to the topic of identity authentication in both the public and the private sector demonstrates the dependency of financial identity theft on developments in other policy arenas, such as terrorism, money laundering, and illegal immigration. Especially, the know your customer provisions present in the USA Patriot Act received the necessary boost to see the light of day since previous attempts to implement such provisions failed due to the lack of support of a focusing event. Simultaneously, however, identity theft itself has also evolved into a vehicle used to target other policy objectives. As the enforcement of the Identity Theft Penalty Enhancement Act demonstrates (see section 3.1.1), the main policy objective is the 'punishment' of illegal immigration through a focus on the usage of 'stolen identities' by them.

Just as September 11, 2001 functioned as a focusing event to provide maximum exposure of the vulnerabilities present in the identification infrastructure, so did ChoicePoint in 2005 with respect to the practices of information brokers. Until then, the existence and practices of data brokers managed to remain out of the public eye and the early warnings issued by interest groups failed to generate sufficient attention for the problematic nature of the industry. When the ChoicePoint story broke in 2005, the protection of personal information and the more general issue of information security became a more pertinent topic on the political agenda. Suddenly, several states began to follow California's lead, which was, after all, the first state to introduce a data security breach notification requirement in 2003.

The Choicepoint story is also indicative for the important role played by the media as an actor who influences the political agenda and the potential for problems to transform into issues of public policy. Kingdon devotes a section to the role played by the media in the agenda setting phase. The impact of media attention is, according to Kingdon, less powerful than generally expected or anticipated. This may be due to "…the press's tendency to cover a story prominently for a short period of time and then turn to the next story, diluting its impact."[1245] Moreover, Kingdon considers the media to function merely as messengers rather than framers. Michael Hill refutes this marginalization of the role of the media during the agenda setting stage.[1246] He claims how "…Kingdon's interpretation of the transmission role of the media is just too facile."[1247] Unlike Kingdon, Hill specifically refers to the importance of when and how problems are reported by the media and their influence on the political attention devoted to the topic.

Still, the dilution of the impact of the media due to its extensive but brief coverage, as Kingdon emphasizes, is noticeable. The media coverage of the stories of victims in the Netherlands led to questions in the Lower House, but generally failed to receive a follow up in the form of a policy initiative. The Ministry of Justice itself noted how there is no direct cause for the criminalization of identity theft in the Netherlands. This was in contrast to the developments in the United

[1245] *Ibid*: 58-59.
[1246] Hill, M. (2009). *The Public Policy Process*. Pearson Education Limited.
[1247] *Ibid:* 167.

States, where such criminalization, as became evident in section 3.1.1, occurred due to the interaction of a victim with his political representative. The presence of a policy entrepreneur therefore became integral to the introduction of a separate criminal provision to combat identity theft.

Much of the agenda setting process, as a result, is reactive and incident-driven. This state of affairs is problematic for such an approach fails to lead to a comprehensive response to the problem, if such a response is even possible. In the United States, the political pressure on the government to act is evident from the combination of factors which provide financial identity theft with its agenda status in the arena of public policy. Its connection to illegal immigration and terrorism enhance its importance and confirm its place on the political agenda. In the Netherlands, the problem is gaining prominence on the political agenda, but is hardly in a similar position as it is in the United States. This, however, may merely be a matter of time as financial identity theft becomes a more spoken about topic at the transnational level.

8.3.2 Crowded Policy Space

In *Speaking Truth to Power*, Aaron Wildavsky asks, "[w]hy do we feel that policy problems never seem to be solved? As knowledge and skill grow in society, why do efforts to control public policies lag behind their ability to surprise us? Why don't organizations that promote public policies seem to learn from their experience? If they do try, why do their actions lead to ever larger numbers of unanticipated consequences?"[1248] "Because", Wildavsky writes, "policy is evermore its own cause, programs depend less on the external environment than on events inside the sectors from which they come."[1249] Rather than suggesting how small solutions are always preferred, Wildavsky attempts to demonstrate how large solutions can displace the original difficulty and as a result create additional problems. This is due to the impact solutions in a single area can have on other policy areas. As Giandomenico Majone notes, "…in an already crowded policy space, solutions beget new problems in the form of policy overlaps, jurisdictional conflicts, and unanticipated consequences."[1250] Financial identity theft, as an issue of public policy, finds itself in the midst of such a crowded policy space. This is in part due to the connection of identity theft with other crimes such as terrorism, money laundering, and human trafficking which leads to the involvement of a myriad of actors. This complicates policy ownership, which in turn influences the direction of the response offered to the problem.

Financial identity theft is also a crowded policy space due to the actors involved in the opportunity structure. While chapter 4 speaks of the state as provider, the state is made up of a myriad of agencies, which all maintain a distinct function. The membership of the Identity Theft Task Force (section 3.5.1) as well as the membership of the steering committee of the Strengthening of the Identification chain in the Public Sector (VIPS) effort in the Netherlands (section 3.5.2) provides an immaculate reflection of the presence of a crowded policy space with respect to financial identity theft. The opportunity structure itself also

---

[1248] Wildavsky, A. (1987). *Speaking Truth to Power: The Art and Craft of Policy Analysis*. London: Transaction Publishers: 62.
[1249] *Ibid.*
[1250] Majone, G. (1989). *Evidence, Argument, & Persuasion in the Policy Process*. New Haven, CT: Yale University Press: 159.

provides a depiction of how certain policies introduced to 'solve' or relieve other problems have in turn evolved into facilitating factors.

8.3.3 Beyond the State

Traditionally, the state maintained a monopoly in its function as protector of the people, especially with respect to the provision of criminal justice. This traditional mindset shines through in chapter 3 which extensively covers various instruments used by the state as protector with respect to financial identity theft. Yet, crime reduction and prevention is no longer an area of society exclusively reserved for the state. Protection or security is ever more a collective responsibility. David Garland eloquently describes this trend in his book *The Culture of Control*. Through the responsibilization theory, the state aims to relocate and redefine responsibilities. As Garland notes, "[i]nstead of addressing crime in a direct fashion by means of the police, the courts and the prisons, this approach promotes a new kind of indirect action, in which state agencies activate action by non-state organizations and actors."[1251] Through this innovative approach, Garland states how the state as an actor of criminal justice is shedding its sovereignty and approximating the notion, as set forth by Michael Foucault, of governmentality. This general approach is apparent in the actions of the state as well as non-government organizations. And the limitations of the traditional criminal justice approach in relation to the challenges associated with the innovative character of financial identity theft in the virtual world certainly develop a persuasive justification for this strategy. This limitation of the state as sole or primary protector therefore influences the available range of countermeasures as well as the state's ability to take direct action to reduce the problem.

Various examples demonstrate the reliance of the state on other actors to carry out its function as protector of the people. The most prominent example is the involvement of the financial services industry in the fight against money laundering. The requirement to maintain an audit trail of accounts opened and transactions carried out by financial service providers has transformed the industry. This transformation, which came as a result of the increased responsibility to actively engage in the fight against money laundering, as well as fiscal fraud and terrorist financing, also meant financial service providers required access to particular instruments, at least in the Netherlands. The push from the financial services industry to gain access to the citizen service number receives justification through its role as participant in the fight against money laundering and terrorist financing. To fulfill a legal mandate, financial service providers, as well as other actors, can in turn also make demands to the state, such as access to or permission to use an identification number or a database. This leads to function creep which is part of the opportunity structure and in turn demonstrates the complexity of 'crime fighting' in contemporary society.

Actors can also profit from the reliance of the state on their existence and practices, and as such remain out of the regulatory reach. This occurs for information brokers, who, as noted in section 8.1.1, cater to the needs of the law enforcement community in the United States and as such find themselves in a privileged position. The necessity of the state then to use the services of the

[1251] Garland (2001): 124.

information brokerage industry in its fight against terrorists and other criminals conflicts with the nature of facilitation of information brokers. Such necessity is borne out of the restrictions placed on the public sector data gathering practices, which lead the law enforcement community to move beyond the state.

In addition to actors in the private sector, the state also appears to include citizens in the group of actors needed to fight crime, or at least financial identity theft. The presence of public awareness campaigns demonstrates the call from the state to its citizens to play a role in the reduction of risks associated with financial identity theft. This also leads to challenges since chapter 6 demonstrates the limited nature of consumers' capacity to protect themselves due to the sophisticated nature of attacks used by perpetrators of financial identity theft.

From a situational crime prevention perspective, the involvement of actors outside of the state is logical since the perspective aims to achieve crime prevention through opportunity reduction which must focus on the entire social context which includes various societal actors. There are, however, limits to the ability of certain actors to contribute to the situational crime prevention and such limits become problematic when the responsibilization strategy induces a transfer of responsibility or liability. Whitson & Haggerty prove critical and state how, "[t]he fact that institutions have knowingly created many of the necessary conditions for identity theft, refused to rectify glaring problems and established bureaucratic structures that give identity theft victimization its characteristic form all suggest that responsibilization measures...are themselves part of a political strategy whereby institutions are divesting themselves of responsibility for the full social and economic costs of the risks they have produced."[1252] This argument receives support through measures taken by ASB Bank, a major bank from New Zealand. ASB Bank emphasizes the responsibility of its individual clients but also changed its terms and conditions in July 2007 to reflect this emphasis. Since July 2007, Internet banking clients without 'proper software security controls' did not receive the right to compensation in case of a successful phishing attack. Hegt notes how, "[t]his has serious implications that go beyond the installation of a virus scanner: ASB Bank enforces their customers to migrate to Windows Vista since full support on Windows XP will soon be dropped by Microsoft. Clearly, this enforcement has serious usability and cost implications for internet banking customers."[1253]

Public awareness campaigns and user education efforts accomplish the responsibilization. This is problematic since the evolution of methods used by perpetrators of financial identity theft demonstrate a decreasing visibility. Such a decrease in visibility translates into a decreasing ability of consumers to control the facilitation of the crime. Herley recognizes the rocky relationship between users and user education.[1254] He opposes previously presented viewpoints which label users as lazy and poorly motivated to act on user education and alter their behavior. In his conclusion, Herley writes, "...users are never offered security, either on its own or as an alternative to anything else. They are offered long, complex and growing sets of advice, mandates, policy updates and tips. These sometimes carry vague and tentative suggestions of reduced risk, never security...much of this advice does nothing to make users more secure, and some

---

[1252] Whitson & Haggerty (2008): 591.
[1253] Hegt (2008): 95.
[1254] Herley, C. (2009). So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. *Proceedings of the 2009 Workshop on New Security Paradigms*.

of it is harmful in its own right. Security is not something users are offered and turn down. What they are offered and do turn down is crushingly complex security advice that promises little and delivers less."[1255]

Even so, the emphasis on consumer responsibility paired with the fear generated about the potential occurrence of financial identity theft proved an incentive for the market to introduce a new industry.[1256] This industry of identity theft prevention services is symbolic for the treatment of the problem of financial identity theft. The mere existence of identity theft prevention services "…acknowledges a significant level of defeat in combating such abuses on the part of industry. The insurers have formulated a program to profit from the very social problem they have helped to create. In this sense, financial identity theft becomes another 'externality' created in the pursuit of corporate profits in the new electronic frontier, a problem that is to be dealt with by 'someone else.'"[1257] This is true for the industry but also for the state, which has indirectly delegated this function as protector, especially in the United States, through its seeming unwillingness or inability to respond to facilitating factors in the financial services industry.

8.3.4 Interdependent Security

Financial identity theft, as the previous chapters as well as the opportunity structure above demonstrate, is inherently a problem of interdependent security for the involvement of various actors is required in an effort to reduce the problem. As a result, the interdependency is evident across different dimensions. There is interdependency among but also within a set of actors. Just as there is interdependency between states themselves. The latter is best depicted through the need for international cooperation in the area of law enforcement. The Council of Europe Convention on Cybercrime demonstrates how its effectiveness rests on the willingness of states to sign and ratify the Convention. The lack of ratification by certain states maintains them as potential data havens and also complicates the efforts of other states who are involved in an investigation.

As for the interdependency between actors, this is best demonstrated by the financial services industry and the comparison between the United States and the Netherlands. For the financial services industry, security is an issue which competes with other core aspects such as convenience and marketing in an effort to maximize profitability. The United States, especially through the opportunity structure revealed above, depicts the consequences of interdependent security within the financial services sector. The competition among players within the sector leads to a focus on convenience and aggressive marketing practices. This is because, as previously noted, an increase in security decreases convenience and can lead to a potential loss of clients. This loss of clients occurs due to the fact that there is no cohesive intention to increase security and such cohesiveness is necessary to overcome the challenge of interdependency. The lack of a cohesive intention then generally means regulation is the necessary instrument to overcome the problem. But this is not always the case. The Netherlands, where the financial

---

[1255] *Ibid:* 11.

[1256] For a more detailed overview of identity theft prevention services see Consumer Federation of America (CFA) (2009). *To Catch a Thief: Are Identity Theft Prevention Services Worth the Cost?*

[1257] Pontell, H.N. & G. Geis (2007). 'New Times, New Crimes: "Blocking" Financial Identity Fraud' in *the Organized Crime Community*. Springer: New York: 54.

services sector is regulated in a more stringent manner, demonstrates the possibility for alternatives. The identification procedures established several decades ago came about through a code of conduct which received good compliance and changed when outside forces, the European Union, issued a directive. The embedding of security in the architecture of Internet banking also came about in negotiation with the Dutch Central Bank. Certainly, as a supervisory organ, the Dutch Central Bank plays an important institutional role, but the engagement of the financial service providers also demonstrates how the smaller scale of the industry assists in its ability to better respond to the challenge of interdependency.

8.3.5 Double Edged Swords

The first part of the opportunity structure provides a brief insight into the potential for double edged swords through the description of how information accumulation is observed as a means to achieve security through risk reduction but can also achieve a state of insecurity. Various instruments introduced in an effort to 'fight' fraud in general and financial identity theft in particular demonstrate this potentially contradictory nature. Jan Grijpink specifically refers to the likelihood of problems associated with the citizen service number initiative, as did others.[1258] Grijpink considers the vulnerability in the current identification infrastructure to be in the predictability of identity check systems.[1259] The current approach to increasing the effort for perpetrators of financial identity theft through enhancing features of documents or other identification tools therefore fails to respond to this vulnerability. And these measures fail to reduce the value of the tools used for identification purposes. Grijpink addresses both of these disadvantages of the current measures introduced and instead proposes a more fundamental change of the infrastructure. Such a fundamental change can come about through making identification procedures less predictable in terms of the manner of the procedure as well as the time and the place. Grijpink labels the more prevalent approach to the reduction of the problem as a choice for simplicity, uniformity, openness, and transparency. Such an approach is very evident through the passage of, for example, the REAL ID Act of 2005 in the United States as well as the approach taken in the European Union which leads to the standardization of identification documents across all member states. This is understandable, according to Grijpink, from a public administration perspective, which is typified by the need for clarity and order; yet, the approach itself is contradictory to the response generally offered by other organisms in nature which is to increase complexity in response to a more complex environment. This occurs through internal differentiation and the diversification of behavior. Better observation is, according to Grijpink, in nature a means to arrive at better control or management of the situation.

Other countermeasures embody the essence of double edged swords. Through the collection of initiatives against money laundering, the state calls for an intensification of surveillance and information accumulation. This, however, leads to the state of information abundance and availability described above as

---

[1258] Prins, J. E. J. (2003). Het BurgerServiceNummer en de strijd tegen Identiteitsfraude. *Computerrecht* (1): 2-3; College Bescherming Persoonsgegevens (2005); Grijpink, J. H. A. M. (2006). Identiteitsfraude en overheid. *Justitiële Verkenningen*, Vol. 32 (7): 37 – 57.

[1259] Grijpink (2006).

part of the opportunity structure. As does the information intensification in the fight against terrorism. Yet, the situational crime prevention identifies surveillance, whether natural, official, or employee, as a means of increasing the effort on the part of the perpetrator. The double edged swords therefore lead to a vicious circle which confirms what Wildavsky states above, that policy is ever more its own cause.

8.3.6 Countering Challenges or Challenging Countermeasures?

The above provides a brief overview of a limited selection of a larger range of challenges faced by policy makers along the path of introducing countermeasures. The place of an issue of public policy on the political agenda invariably colors the response offered by the policy arena. For several years, the United States has maintained identity theft as a priority on its political agenda. This status, however, is in part due to the connection of identity theft to other high level priority items such as illegal immigration and terrorism. Even so, financial identity theft as an issue of public policy profits from the efforts made at the state level which eventually generate sufficient pressure to move into the federal arena. This became evident through the criminalization trend which commenced in the State of Arizona in 1996 and, through the effective usage of a policy entrepreneur, evolved into a federal countermeasure. Data security breach notification legislation appears to follow a similar path. As a result, while the agenda status of financial identity theft remains reactive and incident-driven, the individual states are more prone to react in a rapid manner, which might be the next best thing to a comprehensive approach to the problem.

For the Netherlands, financial identity theft appears to remain in the shadow of the importance placed on look-a-like fraud, which is a document driven type of identity theft often used by illegal immigrants. The focus on a document driven fraud is understandable due to the value of identification documents in the Netherlands, which also explains the emphasis placed throughout the last years to ensure the quality of the document as well as the integrity of the issuance process. Even so, financial identity theft receives more attention through 'intensification' programs introduced in the law enforcement community which specifically target cybercrime, and as such encompass incidents of financial identity theft. The release of data on the financial damage caused by account takeover carried out through Internet banking activities may also satisfy the political craving for a countable problem which can lead to action.

The agenda status of the problem, however, is merely one challenge. The presence of financial identity theft in particular and identity theft in general in a crowded policy space places the potential for countermeasures in a bit of a straightjacket. In response to the criticism offered against data security breach notification, one interviewee responded how other measures might cause more damage, which is certainly a valid concern in light of Wildavsky's notion of policy as its own cause.[1260] The double edged swords, which despite their intention to combat fraud, demonstrate the potential for policy to aggravate rather than reduce the problem.

Moreover, other challenges which influence both the introduction of countermeasures as well as their potential effectiveness include the reliance on

[1260] Interview Technical University Delft, December 3, 2009, Delft.

actors beside the state itself, who do not consider protection of the public as their primary concern or who may simply be unable to defend themselves, as in the case of consumers. As Martin Woollacott argues, "[t]he generalized association of government with the avoidance of risk in wealthy societies is so rooted in expectations, so much a part of both right-wing and left-wing political traditions, that it will survive any trimming of the welfare state. And it is likely to mean that politicians who think that they can rid themselves of responsibility for risk by pushing state functions into the private sphere, or creating 'third party' authorities to carry the can, are going to be gravely disappointed... 'State shedding', or the process by which a more modest state narrows the range of activities and lets its citizens rake risks 'on their own', could turn out to be the biggest illusion of the turn of the century."[1261] The challenge of the involvement of actors beyond the state, namely those in the private sector, is exacerbated by the nature of financial identity theft as a problem of interdependent security which greatly impacts the effectiveness of countermeasures.

8.4 Victims

Stories of victims, both in an individual as well as in a collective sense, often provide a demonstration of the impact of financial identity theft in contemporary society. The countermeasures introduced therefore must also to some extent, be approached, from the perspective of victims. This is especially important since the majority of countermeasures aim to reduce rather than eliminate the problem. This is logical since elimination of the problem is an unrealistic, and perhaps also undesirable, expectation. Such undesirability comes from the intricate connection between the benefits generated from certain facilitating factors, such as efficiency and convenience, which also serve important objectives when approached from a balanced perspective. The elimination of the problem may in turn also lead to the elimination of these benefits. As the brief discussion about the tension between economics and security indicates, the investment in security must be worth the impact in economical terms.

Even so, the achievement of crime reduction as opposed to crime prevention or elimination implies that there shall always be victims. As a result, the response to financial identity theft must focus both on crime reduction as well as crime 'recovery' during the aftermath. The latter is at times lost in the emphasis placed on the former. Through the usage of the fatalistic mantra about how absolute security does, per definition, not exist, the financial services industry aims to void itself of accountability and responsibility when problems arise.[1262] Van Eeten calls this fatalism on someone else's account. This is problematic since the system which generates the risks, whether it concerns the debit card or Internet banking, actually increases the profits for financial service providers due to the reduction of transaction costs. The usage of the system is therefore in the interest of the industry, which ought to then also make an investment in risk reconciliation or risk recovery. For account takeover this means the compensation of funds lost via, for example, a Man in the Browser Attack. Such funds recovery, however, is often subject to interrogation as financial service providers evaluate claims on a case by

[1261] Woollacott, M. (1998). 'The Politics of Prevention,' in J. Franklin (ed.) *The Politics of Risk Society*. Cambridge: Polity Press: 122.
[1262] Van Eeten (2010). *Techniek van de onmacht*. Nederlandse School voor Openbaar Bestuur.

case basis. The initial reaction is to observe the victim as a suspect who has lost the funds as a result of her carelessness. The clever usage of public awareness campaigns and user education instruments as a result completes this problem, as the ASB Bank terms and conditions demonstrate.

8.5 Conclusion

At the end of the road, the conclusion is the moment to stop, turn around, and reflect on the path taken to reach the destination. Looking back at the start, the introduction sketched a brief portrait of the victim that indicated the realistic foundation for the anticipation of identity theft problems in the Netherlands. The existence of victims, albeit a limited number, is indicative of the potential for problems, or at least the presence of fertile grounds for identity theft in the Netherlands. Whether such grounds shall in fact nurture the proliferation of financial identity theft remains difficult to determine in a definitive sense, especially since the background of the developments in the United States demonstrate how years pass before a problem receives official recognition as such. Symptoms, much like the individuals pieces of a puzzle, may exist but no one might be able to provide an official diagnosis of the problem until the problem has become widespread.

As a result, the presence of fertile grounds in the Netherlands must be observed from the perspective of the available nutrients which the crime of financial identity theft needs to escape the soil and reach the surface on its path to maturity. The application of the complementary collection of opportunity theories provided a theoretical lens to observe the experiences in the United States and gage the applicability of such experiences to the situation in the Netherlands. Based on a categorization of actors which together develop a social context which in turn leads to the evolution of an opportunity structure for financial identity theft, there is the start of an understanding about how financial identity theft relates to routine daily activities in contemporary society. The opportunity structure depicts the differences between the United States and the Netherlands, and also demonstrates how the underlying mechanisms carry an 'explanatory power' to comprehend such differences. A certain share of such differences relates to uncontrollable features of both countries such as the distinction in scale and size. Other differences prove to be an expression of culture and style of governance, which in turn influence the presence of nutrients to facilitate financial identity theft.

The absence of certain facilitating factors in the Netherlands, as opposed to the United States, might be interpreted as a promising feature of this research. And certainly such an absence ought to put into perspective any potential hysteria about the outbreak of financial identity theft across the country. Still, as became evident in the United States, early warnings about particular features in society, which demonstrate a likelihood to engage in function creep or fall 'victim' to the enticing nature of convenience, should be observed from a distance. For if we remain too close to the individual pieces, we shall never be able to observe the entire puzzle.

As the 9/11 Commission acknowledged in retrospect, the system was blinking red but everyone failed to connect the dots. There is a chance the same might happen in the Netherlands, despite the absence of certain facilitating factors which nurture financial identity theft in the United States. The importance of attention

devoted to early warnings rests in the limited nature of countermeasures introduced once the problems actually surface. Countermeasures which increase the effort and increase the risk can restrict the provision of nutrients, but will not kill the poison ivy that is financial identity theft. For both categories of countermeasures are inherently 'reactive' which complicates their nature as a means to prevent crime. The 'reactive' nature of countermeasures comes as a result of the neglect offered to early warnings about developments which maintain the potential to lead to a facilitating factor for financial identity theft. In retrospect such early warnings prove to be a foreshadowing of the problems which surface in due time. The general message which must be taken away from the warnings is a sense of caution about developments which embrace an unbalanced approach to potentially conflicting interests. However much token attention is devoted to the notion of balance, an actual balance is rarely achieved in practice. The importance of function creep and the cost of convenience, as well as the transformation from elite to mass and the obsession with information in contemporary society reflect how the aim to balance between the interests of privacy, security, and convenience is a thought remembered but an idea unrealized in the enthusiasm of progress. The grounds facilitating identity theft, then, will remain fertile indeed.

SUMMARY

When identity theft originally emerged as a problem of public policy in the United States, during the last decade of the twentieth century, the rest of the world was still vast asleep. This changed several years later as other countries awakened to similar problems and a sense of potential urgency surrounding the topic of identity theft began to spread. Identity theft, especially as a result of advances made with regard to digital technology, became a threat worthy of social and political attention. Such interest in the 'novel' phenomenon led to many questions. The dominant discussions primarily focused on the lack of a standard definition and the necessity for prevalence data in an effort to assess the size and subsequent importance of the problem. Neither question proved easy to answer. Despite the extensive consideration granted to the importance of prevalence data and the establishment of a standard definition, other significant and perhaps more fundamental questions hovered in the background. The existence of financial identity theft in the United States, and its gradual potential spread to other areas of the world, increases the need to understand how identity theft occurs and how perpetrators of the crime manage to take advantage of developments within contemporary society. This book aims to provide such an answer through its central research question:

How do states, financial service providers, consumers, and others facilitate the occurrence of financial identity theft in the United States and the Netherlands? And what are the implications for existing countermeasures and how do these fit into the situational crime prevention framework?

The in-depth analysis of each actor provides the basis for the development of an opportunity structure, which serves as an overarching framework for previously identified facilitating factors. The four elements of the opportunity structure cover both the first and second stage of financial identity theft. This distinction is also the red threat throughout the book to categorize facilitating factors. The first stage of financial identity theft concerns the collection of personal information or other identification instruments, whereas the second stage revolves around the actual use, or better yet abuse, of the previously collected information or instruments for financial gain.

Information: Abundance, Availability, and Accessibility

The first aspect of the opportunity structure logically focuses on the facilitation of the first stage of financial identity theft. This is the element of information and its abundance, availability, and accessibility. The abundance of information is mainly the result of the elimination of 'physical' obstacles with respect to storage space in the virtual world. The collection and storage of information have as a result experienced enormous growth. This is evident in the analysis of both the state, as protector and provider, as well as in the examination of other actors such as information brokers and payment processors.

Besides the sheer ability to increase the collection of information and its storage, actors, especially the state as protector, have also expressed an enhanced necessity to engage in such record-keeping activities. This is mainly the result of the focus on information collection as a means to reduce risks and in turn achieve

a sense of 'collective security.' The events of September 11, 2001 and the overall fight against terrorism increased the desire of the state, both the United States and the Netherlands, to accumulate more information. This trend to increase information collection as an instrument to reduce risks and subsequent crime maintains historical roots, as became evident through the comprehensive background analysis of anti-money laundering legislation. The perceived necessity for information also provides an impetus for the information brokerage industry to evolve and subsequently flourish. Whereas much information collection and storage occurs as a means to achieve collective security, such activities in turn also facilitate a (potential) state of individual *insecurity*. Such a state of individual insecurity can surface when the information collected and stored is accessible for perpetrators of financial identity theft. This became especially apparent through the onset of media reports about data security breaches such as ChoicePoint in 2005 which illustrated how the information brokerage industry along with other organizations inside and outside of the public sector proved to be an attractive target for perpetrators of financial identity theft.

Just as the collection and storage of information increased, so did the ability for individuals to provide and share information. For consumers such an increase is evident through the usage and popularity of social media applications. This also made and continues to make information more available, especially via the Internet.

The abundance and availability of information are important; yet, the accessibility of information, in particular personal information, is a vital aspect of the overall facilitation of the first stage of financial identity theft. The aspect of accessibility has also been greatly influenced through the evolution of digital technology. For the state as provider, in particular, the accessibility of information became a prime topic of development. The most apparent example originates from the Netherlands where the government decided to make a central version of the Municipal Personal Records Database available via the Internet. This trend to allow access to a database in the virtual world also enhances its vulnerability for potential intrusion.

The increase in the availability and accessibility of personal information also becomes more problematic due to the enhanced value and applicability of such information in contemporary society. This is primarily due to the move away from face to face and onto digital transactions, where information has become a vital aspect of routine activities. This transition or function creep is a recurring feature throughout other facilitating factors and as such another aspect in the overall opportunity structure.

Function Creep

Function creep is a phenomenon which collectively captures a number of different aspects which lead to the facilitation of financial identity theft. The first example is the increasing usage and value of personal information in contemporary society. Perpetrators of financial identity theft acknowledge how personal information is like the key to the kingdom, since such information opens doors to financial assets.

Moreover, several (identification) instruments introduced by the state as provider experienced an expansion of applicability or 'functions' beyond their original intent. The most apparent example of function creep with respect to the

facilitation of financial identity theft is the usage of the Social Security Number in the United States. Its historical background demonstrates how the incremental expansion of usage led to a state of affairs where the number is valuable yet readily available and accessible. The value of the number rests in its usage by both the public and the private sector for verification purposes. A similar pattern, at least in terms of availability and accessibility, also surfaced in the Netherlands. The historical background of the citizen service number, and its predecessor the social-fiscal number, demonstrate how the applicable uses of the number expanded beyond its original intent and how the desire for increased access by other actors, especially the private sector, continues to exist.

The emergence of function creep is also demonstrated by the increased reliance on identification documents. The introduction of both the passport and the driver's license occurred with a specific intent; yet, this original purpose has since been buried by the plethora of situations where individuals can and often must use these documents. The function creep raises the value of identification documents and as a result enhances the need to strengthen the issuance process as well as the quality of the product. Through a historical analysis, it has become evident how both of these 'security' aspects remain particularly challenging. The Netherlands carries a turbulent history with respect to the development of a passport which proved resistant to fraud, whereas the events of September 11, 2001 heightened the awareness in the United States about the problems surrounding their issuance process with respect to driver's licenses.

The overarching 'instrumental' function creep can also be extended to the functionality of the computer and the mobile phone which, in contemporary society, have significantly expanded and as a result also led to an expansion of opportunities. Much like the stretch of an elastic band, such an expansion of functionality increases the tension and places a higher pressure on the security of the instrument to prevent it from 'snapping.'

From Elite to Mass

The historical analysis of the credit card in particular demonstrates how a transformation occurred, at least in the United States, from a product of the elite to a product of the masses. This transformation also became evident through the historical analysis of the passport, which originally maintained an air of privilege but transformed into an obligation. This transformation is important on two different dimensions. First, such a transformation changes the scale of the feature and therefore increases the applicable population. This increase also translates into an increase of suitable targets for perpetrators of crime. Second, a transformation from elite to mass means the population which can gain access or entry to a particular tool or feature also increases, which often means the entry requirements decrease and the acquisition of clients becomes more aggressive. This is especially apparent in the historical background of the credit card where the increased competition within the industry also increased the need for clients. Through the increased desire to gain as many clients as possible, those active in the industry reduced the threshold for applications and became more willing to issue credit cards on a large basis. Despite the elimination of unsolicited credit cards, the application process remains an issue which emphasizes mass acquisition of clients through focusing on speed and convenience. This in turn leads to the (potential) facilitation of financial identity theft.

The Cost (and Profit) of Convenience

Convenience is an issue which is emphasized throughout the decision making process of various actors, from states to financial service providers. Convenience, however, remains the enemy of security. For consumer or client convenience also becomes criminal convenience, which facilitates financial identity theft. For the state as provider convenience is an important aspect during the development of electronic government applications. It is in the interest of the state after all to keep the threshold for enrollment low to ensure as many citizens as possible begin to use e-government applications. The mass usage of e-government applications is an objective of the state in an effort to reduce administrative burdens and increase the efficiency of its operations. Both the United States and the Netherlands have started speaking of customers as opposed to citizens, which again enhances the emphasis placed on convenience in the delivery of their services.

Along similar lines, financial service providers also focus on convenience as a means to maximize the number of clients and profits. The acquisition and application process of the credit card industry in the United States illustrates this emphasis on convenience. Such an emphasis on convenience returned when the financial services sector began to use the digital world for its transactions. Despite the existing common consensus on the necessity to enhance the security aspect of digital transactions, nearly all banks decided to install a mere one-factor authentication system, which proved vulnerable to intrusion, but allowed the providers to maintain a low threshold, which in turn increased client usage. For the financial services sector in the Netherlands the story is different mainly due to the existing solidarity among a small number of actors within the industry. As a result, the lack of emphasis placed on convenience through the introduction of a two-factor authentication mechanism for electronic banking, for example, does not carry any negative consequences since the enhanced security features are incorporated by all banks, which prevents the potential loss of clients since there are no alternatives.

Countermeasures

The development of an overarching opportunity structure can in turn serve as a tool of reflection with respect to existing and proposed countermeasures. These countermeasures are categorized according to the situational crime prevention framework, which provides various types of opportunity reduction strategies. The first two, increasing the effort and increasing the risk, appear to be the most applicable types of reduction strategies with respect to the facilitation of financial identity theft. Both of these categories can apply to the first as well as the second stage of the crime. For the first stage, increasing the effort mainly occurs through reducing the opportunities for attaining personal information. Applicable existing countermeasures include public awareness campaigns which aim to make consumers more aware in an attempt for them to better safeguard their personal information. Due to the increased sophistication of attacks, the ability of consumers to arm themselves against outside infiltration is slowely but surely diminishing. The state as protector has also implemented data security breach notification requirements which try to increase the effort in two ways. First, consumers receive a notification of an organization when their data has been (potentially) compromised. This notification and awareness ought to serve as a

means for consumers to take action, which is in light of the compromised status of the data a complicated feat. The second aim is to provide an incentive for organizations to improve their information security practices, and as such reduce opportunities for perpetrators of financial identity theft to gain access to the personal information maintained by the respective organization. The focus on incentives is promising since the potential costs associated with reputation damage for an organization as a result of the notification is a powerful instrument to improve security.

Besides increasing the effort to obtain personal information, both governments have also introduced measures to complicate the attainment of identification documents. This occurs, for example, through changes made to the issuance process of such documents. In the United States, the passage of the REAL ID Act aims to improve both the quality of the document as well as its issuance process. For the Netherlands, the law enforcement community is working with municipalities to strengthen the issuance process and as such increase the effort needed from perpetrators of financial identity theft to obtain a passport or driver's license.

Other measures aim to increase the effort required to accomplish the second stage of financial identity theft. These include changes made to authentication schemes for electronic banking, such as SMS authentication and the substitution of an EMV chip for the black stripe on the back of debit cards. Attempts by merchants to reduce opportunities for financial identity theft include requesting the CVC code and using the 3D Secure system.

Besides increasing the effort, existing countermeasures also aim to increase the risk. This occurs through the incorporation of the criminal justice system as a means to increase the risk of being caught which in turn theoretically serves as a deterrent. Whereas the United States officially criminalized identity theft in 1998, the Netherlands instead decided to rely on existing criminal law in the fight against identity theft. Important to note, however, is how the Dutch government intensified the fight against cybercrime and financial economic crime which also provides benefits for the reduction of financial identity theft.

Conclusion

Based on a categorization of actors which together develop a social context which in turn leads to the evolution of an opportunity structure for financial identity theft, there is the start of an understanding about how financial identity theft relates to routine daily activities in contemporary society. The opportunity structure depicts the differences between the United States and the Netherlands, and also demonstrates how the underlying mechanisms carry an 'explanatory power' to comprehend such differences.

The absence of certain facilitating factors in the Netherlands, as opposed to the United States, might be interpreted as a promising feature of this research. Still, as became evident in the United States, early warnings about particular features in society, which demonstrate a likelihood to engage in function creep or fall 'victim' to the enticing nature of convenience, should be kept in mind.

The importance of attention devoted to early warnings rests in the limited nature of countermeasures introduced once the problems actually surface. Countermeasures which increase the effort and increase the risk can restrict the provision of nutrients, but will not kill the poison ivy that is financial identity theft.

For both categories of countermeasures are inherently 'reactive' which complicates their nature as a means to prevent crime. The general message which must be taken away from early warnings is a sense of caution about developments which embrace an unbalanced approach to potentially conflicting interests. However much token attention is devoted to the notion of balance, an actual balance is rarely achieved in practice. The importance of function creep and the cost of convenience, as well as the transformation from elite to mass and the obsession with information in contemporary society reflect how the aim to achieve a balance between the interests of privacy, security, and convenience is a thought remembered but an idea unrealized in the enthusiasm of progress. The grounds facilitating identity theft, then, will remain fertile indeed.

SAMENVATTING

Toen identiteitsdiefstal aan het einde van de twintigste eeuw in de schijnwerpers van de Verenigde Staten kwam te staan lag de rest van de wereld nog rustig te slapen. Een verontrustend gevoel van urgentie over het fenomeen fungeerde enkele jaren later als een alarmsignaal voor andere landen, zowel binnen als buiten de Europese Unie. Inmiddels heeft identiteitsdiefstal zich ontpopt tot een bedreiging die politieke en maatschappelijke aandacht verdient en krijgt. Deze belangstelling heeft tot moeilijk te beantwoorden vragen geleid, over aard en omvang van het fenomeen in het bijzonder. Het ontbreken van een standaard- of algemeen geaccepteerde definitie en de noodzaak om statistische gegevens over de omvang van het fenomeen te krijgen, overheersen daarom vaak het debat. Ondanks de aandacht voor het definitievraagstuk en de drang naar statistieken, spelen op de achtergrond fundamentelere vragen. Het bestaan van identiteitsdiefstal in de Verenigde Staten en de (mogelijke) geleidelijke verspreiding van het probleem naar andere delen van de wereld versterken de noodzaak om te begrijpen hoe identiteitsdiefstal plaatsvindt en hoe daders misbruik weten te maken van maatschappelijke ontwikkelingen. Dit proefschrift beoogt daarom antwoord te geven op de volgende centrale onderzoeksvraag:

Hoe faciliteren overheden, financiële dienstverleners, consumenten en anderen financiële identiteitsdiefstal? En wat voor implicaties heeft dit voor bestaande maatregelen en hoe passen deze binnen het kader van 'situational crime prevention'?

De uitgebreide analyse van elke actor vormt een goede basis voor het ontwikkelen van een overkoepelende gelegenheidsstructuur, waarin alle faciliterende factoren terugkeren en gekoppeld worden aan hun bredere sociale context. Bij het in kaart brengen van een gelegenheidsstructuur is het goed om een onderscheid te maken tussen de eerste en de tweede fase van identiteitsdiefstal. Dit onderscheid loopt tevens als rode draad door het gehele boek. De eerste fase van identiteitsdiefstal bestaat uit het verkrijgen van persoonsgegevens of instrumenten die gebruikt kunnen worden voor identificatie, terwijl de tweede fase betrekking heeft op het gebruiken, of beter gezegd misbruiken, van deze gegevens of instrumenten om een bepaald voordeel te behalen. In dit boek ligt de nadruk op financieel gewin, oftewel op financiële identiteitsdiefstal.

Informatie: Overvloed, Beschikbaarheid en Toegankelijkheid

Het eerste aspect van de gelegenheidsstructuur hangt logischerwijs samen met de eerste fase van identiteitsdiefstal. Dit is het aspect van informatie en richt zich vooral op de overvloed, beschikbaarheid en toegankelijkheid van gegevens. De huidige overvloed van gegevens is voornamelijk het gevolg van het ontbreken van fysieke barrières met betrekking tot opslagruimte in de virtuele wereld. Het verzamelen en vervolgens opslaan van gegevens heeft daarom een enorme vlucht genomen. Dit komt nadrukkelijk naar voren in de analyse van de staat, als beschermer en dienstverlener, maar ook bij andere partijen, waaronder informatiehandelbureaus. Naast de mogelijkheid om steeds meer gegevens te verzamelen en op te slaan hebben partijen, de staat als beschermer in het bijzonder, ook de noodzaak hiervan benadrukt. Deze noodzaak komt voort uit de overtuiging dat het verzamelen en opslaan van gegevens een geschikt middel is om

risico's te verkleinen en om bij te dragen aan 'publieke veiligheid', of althans het veiligheidsgevoel van burgers en consumenten. De gebeurtenissen van 11 september 2001 en de algemene strijd tegen terrorisme hebben, zowel in de Verenigde Staten als in Nederland, de behoefte aan het verzamelen en opslaan van gegevens versterkt. Deze tendens om het verzamelen en opslaan van gegevens in te zetten als middel om risico's te verkleinen en misdaad te verminderen is al enige tijd aanwezig, zoals bleek uit een analyse van de achtergrond van anti-witwaswetgeving. Terwijl het verzamelen en opslaan van gegevens vaak wordt ingezet als middel om publieke veiligheid te bevorderen, kunnen deze activiteiten echter ook een potentiële staat van individuele onveiligheid faciliteren. Dit kan gebeuren als de opgeslagen gegevens toegankelijk zijn voor identiteitsdieven door haperende informatiebeveiliging. Dit toont aan hoe de overvloed en de beschikbaarheid van gegevens belangrijk zijn, maar hoe de toegankelijkheid van gegevens, in het bijzonder persoonsgegevens, tevens een cruciaal aspect is voor het faciliteren van identiteitsdiefstal. Deze constatering wordt versterkt door berichten in de media over het 'lekken' van gegevens bij informatiehandelbureaus, zoals ChoicePoint in 2005. De berichtgeving over ChoicePoint geeft aan hoezeer de industrie van informatiehandelbureaus in de Verenigde Staten een aantrekkelijk doelwit vormt voor identiteitsdieven. Mede omdat het bestaan van deze industrie de toegankelijkheid van persoonsgegevens vergroot.

Naast de toename in het verzamelen en opslaan van gegevens is ook de mogelijkheid om gegevens met anderen te delen gegroeid. Dit is vooral relevant bij consumenten, onder andere door de populariteit van sociale netwerken waar steeds meer mensen informatie delen en dus beschikbaar maken voor anderen. Hierdoor worden persoonsgegevens steeds breder en makkelijker beschikbaar, met name via het Internet.

Los van de toegenomen beschikbaarheid en toegankelijkheid van persoonsgegevens is ook de waarde van gegevens gestegen door de opkomst van digitale transacties en activiteiten. De overgang van fysieke naar digitale transacties vergt andere middelen om iemands identiteit te verifiëren. Hierdoor stijgt de waarde van persoonsgegevens, aangezien deze op meerdere fronten inzetbaar zijn. Dat leidt tot uitbreiding van toepassingen die we ook zien bij de analyse van andere factoren, en speelt daarom een belangrijke rol binnen de gelegenheidsstructuur.

Function Creep

Function creep, of het uitbreiden van toepassingen buiten het oorspronkelijke doel, is een fenomeen dat meerdere faciliterende factoren verenigt. Ten eerste betreft dat het hiervoor geschetste toenemende gebruik en de waarde van persoonsgegevens. Identiteitsdieven begrijpen bijzonder goed hoe persoonsgegevens in de huidige maatschappij vergelijkbaar zijn met de sleutel tot de schatkist. Verder zijn de toepassingen van (identificatie) instrumenten die de door de staat als dienstverlener zijn geïntroduceerd, regelmatig uitgebreid. Het meest in het oog springende voorbeeld daarvan is het gebruik van het Social Security Number in de Verenigde Staten. Een historische schets van dit nummer laat zien hoe de geleidelijke uitbreiding van de toepassing ervan heeft geleid tot de huidige situatie, waarin het nummer alom beschikbaar en toegankelijk maar ook zeer waardevol is. Het nummer wordt gebruikt als verificatiemiddel in de publieke en de private sector en heeft daardoor een waardevolle maar ook kwetsbare positie

verworven. In Nederland zien we in historisch perspectief een soortgelijk patroon, tenminste op het vlak van de beschikbaarheid en de toegankelijkheid van het identificatienummer. Een historische schets van het huidige burgerservicenummer en haar voorganger het sociaal-fiscaal nummer laat zien hoe de toepasbaarheid in de loop der jaren is gegroeid en haar oorspronkelijke functie ver voorbij is gestreefd. Daarnaast is ook duidelijk geworden hoe toegang tot het nummer, in het bijzonder door de private sector, een gewild object is waardoor de uitbreiding in termen van beschikbaarheid en toegankelijkheid in de toekomst nog verder zou kunnen gaan.

Het fenomeen van function creep is ook te zien in de toenemende afhankelijkheid van identificatiedocumenten. Zowel het paspoort als het rijbewijs zijn ooit met een specifiek doel tot stand gekomen. Dit specifieke doel – het bewijzen van iemands toelaatbaarheid om landsgrenzen over te gaan respectievelijk een auto te besturen – is echter in de afgelopen decennia steeds meer vervaagd, doordat er uiteenlopende toepassingen zijn bijgekomen waarvoor beide documenten gebruikt worden. Deze uitbreiding van toepassingen heeft wederom als gevolg dat het document stijgt in waarde en aantrekkelijker wordt als doelwit van identiteitsdieven, waardoor er meer druk komt te staan op de kwaliteit van het product en het uitgifteproces.

Door middel van een historische analyse is duidelijk geworden hoe de beveiliging van identiteitsdocumenten een uitdaging blijft voor overheden, zowel in de Verenigde Staten als in Nederland. De turbulente geschiedenis van Nederland met betrekking tot het paspoort geeft aan hoe de fraudegevoeligheid van het document lange tijd fungeerde als plaaggeest voor de overheid. Inmiddels, mede onder invloed van de Europese Unie, is het Nederlandse paspoort weerbaarder geworden tegen vroegere kwetsbaarheden. Voor de Verenigde Staten hebben de gebeurtenissen van 11 september 2001 duidelijk gemaakt hoe kwetsbaar het uitgifteproces van rijbewijzen is. Het verband met terrorisme vergrootte het bewustzijn van de noodzaak om rijbewijzen, zowel het product als het uitgifteproces, beter te beveiligen.

Verder neemt de functionaliteit van de computer en de mobiele telefoon nog steeds enorm toe. Door de uitbreiding van mogelijkheden met deze instrumenten neemt ook de kwetsbaarheid toe, waardoor de beveiliging verder onder druk komt te staan om mogelijke aanvallen tegen te houden. Over het algemeen is het meer en meer gebruiken van een bestaand instrument een vaak voorkomende tendens, aangezien dit meestal het gebruikersgemak vergroot en tevens een grote mate van efficiëntie met zich meebrengt.

Van elite naar massa

De in deze studie uitgevoerde historische analyse van de credit card geeft aan hoe het instrument, tenminste in de Verenigde Staten, in de loop der tijd een omslag heeft gemaakt van een elitair product naar een product voor het bredere publiek. Deze vertaalslag komt ook naar voren in een historische analyse van het paspoort, wat van oudsher primair een voorrecht was en pas veel later veranderde in een verplichting. Deze verschuiving van elite naar massa is belangrijk om twee redenen. Allereerst leidt deze verandering tot een schaalvergroting, waardoor de hoeveelheid potentiële slachtoffers exponentieel toeneemt. Ten tweede, en dit geldt in het bijzonder voor de credit card, heeft het gevolgen voor de toegankelijkheid van het product. De standaarden waar potentiële cliënten aan

moeten voldoen dalen omdat het een primaire drijfveer is voor financiële dienstaanbieders om zoveel mogelijk cliënten binnen te halen om winst te maximaliseren. Hiermee gaat het fraudegevoelige karakter omhoog. Dat blijkt nadrukkelijk uit verhalen over credit cards die bedrijven hebben verleend aan honden, kinderen en anderen waarvan duidelijk had moeten zijn dat deze geen credit card hadden moeten kunnen krijgen. In het spanningsveld tussen zorgvuldige identificatieprocessen bij de uitgifte van credit cards enerzijds en klantenpotentieel in een sterk concurrerende markt anderzijds kiezen dienstverleners in de Verenigde Staten vaakvoor het laatste ten koste van het eerste.

De bijwerking van (gebruikers)gemak

Gebruikersgemak krijgt bij besluitvormingsprocessen over digitale ontwikkelingen veel aandacht, zowel bij overheden als bij financiële dienstverleners. Gemak is echter vaak een vijand van beveiliging. Dit wordt in deze studie mede geïllustreerd door het feit dat gebruikersgemak zich vaak vertaalt naar gemak voor de criminele wereld, omdat laagdrempeligheid voor gebruikers vaak ook misdadige activiteiten faciliteert. Voor de staat als dienstverlener is gemak een belangrijk aspect bij het ontwikkelen van applicaties voor de elektronische overheid. De overheid heeft er per slot van rekening zelf belang bij dat burgers gebruik gaan maken van de mogelijkheden van elektronische publieke dienstverlening. Grootschalig gebruik van de elektronische overheid is een doel voor de overheid omdat het kan leiden tot lastenvermindering en de efficiëntie kan vergroten. De Verenigde Staten en Nederland zijn in de context van e-overheid beiden gaan spreken over klanten of consumenten in plaats van burgers, wat de nadruk op gebruikersgemak en het dienstverlenende karakter van de overheid heeft versterkt.

Op een soortgelijke manier hebben financiële dienstverleners ook de nadruk gelegd op gemak, om op deze manier zoveel mogelijk klanten te bereiken en winst te behalen. De acquisitie van klanten en het aanmeldproces binnen de credit card-industrie in de Verenigde Staten geeft aan hoeveel nadruk er ligt op gebruikersgemak om dit doel te verwezenlijken. Deze afweging zien we terug in het systeem van elektronisch bankieren waarbij in de Verenigde Staten veelal is gekozen voor een authenticatiemechanisme op basis van één factor (zoals een wachtwoord), om de drempel voor toetreding zo laag mogelijk te houden. Dit ondanks de breed gedragen mening dat 1-factor-authenticatie bij financiële transacties onvoldoende beveiliging biedt. In de financiële dienstverlening in Nederland tekent zich een ander beeld af. Daar heeft de kleinschaligheid van de sector, in het bijzonder met betrekking tot de betrokken partijen, ertoe geleid dat voldoende solidariteit bestond om samen een hoger beveiligingsniveau te introduceren, waarbij authenticatie plaatsvindt op basis van meerdere factoren (zoals een wachtwoord én een apparaatje of TAN-codes). Door deze collectieve benadering bleef het risico van overloop van klanten uit, waardoor het lagere gebruikersgemak, anders dan in de VS, geen invloed had op de concurrentiepositie.

Samenvattend kan de gelegenheidsstructuur geschetst worden als een omgeving waarin de maatschappelijke voordelen van bepaalde ontwikkelingen, in het bijzonder met betrekking tot digitale mogelijkheden, tevens kansen heeft geschept voor identiteitsdieven. Dit is belangrijk om te benadrukken omdat het aangeeft

hoe beperkt wellicht de mogelijkheden zijn voor (effectieve) maatregelen om de misdaad te verminderen.

Maatregelen

De ontwikkeling van een overkoepelende gelegenheidsstructuur kan vervolgens fungeren als een spiegel voor de maatregelen die diverse actoren reeds getroffen hebben ter bestrijding van identiteitsdiefstal. Deze maatregelen kunnen geplaatst worden in het theoretische model van 'situational crime prevention'. De eerste twee technieken/strategieën van dit model, het bemoeilijken van de misdaad en het verhogen van het risico voor daders, zijn de meest relevante categorieën voor identiteitsdiefstal. Beide categorieën zijn van toepassing op de eerste en de tweede fase van identiteitsdiefstal.

Voor de eerste fase zijn met name relevant de maatregelen die zich richten op het reduceren van mogelijkheden om persoonsgegevens te bemachtigen. Getroffen maatregelen in deze categorie zijn onder andere voorlichtingscampagnes. Deze campagnes hebben als primair doel om burgers bewust te maken van het gevaar van identiteitsdiefstal, zodat zij voorzichtiger en terughoudender omgaan met hun persoonsgegevens. Door de steeds geavanceerdere methodes van identiteitsdieven worden de mogelijkheden van burgers om zich te beschermen, echter steeds beperkter. Andere maatregelen die de overheid als beschermer heeft getroffen, beogen om persoonsgegevens bij de private sector beter te beschermen. Een hippe maatregel is tegenwoordig een meldplicht voor organisaties die persoonsgegevens 'gelekt' hebben of voorvallen kennen waarbij deze gegevens mogelijk gecompromitteerd zijn. Deze meldplicht heeft twee doelen. Ten eerste wordt beoogd dat burgers, wanneer zij op de hoogte worden gesteld van het incident, zich kunnen wapenen tegen de mogelijke gevolgen. Dit doel is moeilijk te verwezenlijken, aangezien burgers nauwelijks invloed kunnen uitoefenen op het plegen van identiteitsdiefstal wanneer de gegevens inmiddels al in kwaadaardige handen liggen. Het tweede doel is om organisaties te motiveren om hun informatiebeveiliging te verbeteren. De theorie is dat dit gebeurt omdat het melden van een incident van gegevensverlies kan leiden tot reputatieschade, waardoor een investering in betere informatiebeveiliging meer voordelen heeft in een kosten-baten-analyse.

Verder richten overheden zich op het bemoeilijken van het verkrijgen van een identificatiebewijs, onder andere door het introduceren van veranderingen in het uitgifteproces. Op dit vlak heeft in Nederland de politie toenadering gezocht tot de gemeentes om samen het uitgifteproces te versterken door toezicht te houden op de aangifte van vermiste of verloren documenten. In de Verenigde Staten heeft de federale overheid geprobeerd om via de REAL ID Act het uitgifteproces van officiële documenten te stroomlijnen en versterken.

Andere maatregelen spitsen zich meer toe op het bemoeilijken van de tweede fase van identiteitsdiefstal. Hieronder vallen verbeteringen in het authenticatiesysteem van elektronisch bankieren, maar ook het vervangen van de zwarte, magnetische strip aan de achterkant van een pinpas (die kwetsbaar is voor 'skimmen') door een EMV-chip. Verder hebben webhandelaren ook geprobeerd identiteitsdiefstal te bemoeilijken door bij transacties op afstand te vragen naar de CVC-code op de achterkant van de credit card.

Naast het bemoeilijken van identiteitsdiefstal in operationele zin, beogen andere maatregelen de risico's te verhogen voor misdadigers – de tweede strategie

in het 'situational crime prevention'-model. Dit gebeurt aan de hand van een betere inzet van politie en justitie, onder andere om de pakkans te vergroten en daardoor daders te ontmoedigen om identiteitsdiefstal te plegen. De Verenigde Staten heeft in dat licht er in 1998 voor gekozen om identiteitsdiefstal specifiek strafbaar te stellen, zodat het probleem in beeld kwam bij de politie en justitie er gericht op kon vervolgen. Nederland heeft daarentegen besloten om gebruik te maken van bestaande wetgeving binnen het strafrecht, waaronder identiteitsdiefstal ook kan worden geschaard, maar heeft daarentegen wel aandacht geschonken aan het intensiveren van de aanpak van cybercrime en financieel economische criminaliteit.

Conclusie

In deze studie zijn alle partijen beschreven en geanalyseerd die samen de sociale context creëren waarbinnen een gelegenheidsstructuur onstaat voor identiteitsdiefstal: de overheid als beschermer, de overheid als dienstverlener, financiële dienstverleners, overige bedrijven, consumenten en tussenpersonen. Daarmee is een begin gemaakt om te begrijpen hoe identiteitsdiefstal zich verhoudt tot de dagelijkse activiteiten in de huidige maatschappij. Het zijn immers de dagelijke activiteiten van alle actoren die gelegenheden scheppen – of juist kansen verkleinen - om identiteitsdiefstal te plegen. De aldus beschreven gelegenheidsstructuur geeft verschillen weer tussen de Verenigde Staten en Nederland en illustreert ook hoe achtergrondverhalen een verklaring kunnen geven voor deze verschillen. Gebleken is dat bepaalde faciliterende factoren die in de Verenigde Staten prominent aanwezig zijn, ontbreken in Nederland. Men zou dat kunnen interpreteren als een optimistisch vooruitzicht (voor Nederland), maar zoals duidelijk geworden is uit de analyse van de Amerikaanse bevindingen, is het van wezenlijk belang alert te zijn op bepaalde aspecten binnen de maatschappij die een voorbode zijn van veranderingen in de gelegenheidsstructuur. Zulke aspecten zijn de neiging tot function creep of het leggen van een overmatige nadruk op de aantrekkelijkheid van gebruiksgemak. Dergelijke 'vroege signalen' van naderende veranderingen in de gelegenheidsstructuur zijn belangrijk om in het achterhoofd te houden bij vele besluitvormingsprocessen in de publieke alsook in de private sector.

Het is belangrijk om aandacht te schenken aan vroege signalen en om bevindingen uit andere landen als waarschuwingen voor ogen te houden. Dat belang is des te groter omdat tegenmaatregelen maar in beperkte mate invloed kunnen uitoefenen op identiteitsdiefstal als het probleem eenmaal aanwezig is. De algemene boodschap die voortvloeit uit een vroeg signaleringssysteem is dat men bij uitstek moet oppassen bij ontwikkelingen die op een onevenwichtige manier omgaan met belangenconflicten. Hoeveel aandacht er ook besteed wordt aan het idee dat belangen evenwichtig moeten worden afgewogen, een echt evenwicht is zelden terug te vinden in de praktijk. De in deze studie gevonden faciliterende factoren, van function creep, nadruk op gebruikersgemak en een verschuiving van elite naar massa tot de informatieobsessie in de huidige maatschappij, vormen signalen van een gelegenheidsstructuur voor identiteitsdiefstal. Wanneer deze signalen genegeerd worden bij complexe belangenafwegingen in besluitvormingsprocessen, zal er vruchtbare grond zijn voor identiteitsdiefstal om in te woekeren.

REFERENCES

Abagnale, F. W. (2007). *Stealing your life: The ultimate identity theft prevention plan*. New York: Broadway.

Abu Rajab, M., Zarfoss, J., Monrose, F. & A. Terzis (2006). A Multifaceted Approach to Understanding the Botnet Phenomenon. *Proceedings of ACM SIGCOMM/USENIX Internet Measurement (IMC)*: 41-52.

Acohido, B. & J. Schwartz (2008). *Zero-Day Threat: The Shocking Truth of How Banks and Credit Bureaus Help Cyber Crooks Steal Your Money and Identity*. New York: Union Square Press.

Acquisti, A. & R. Gross (2009). Predicting Social Security numbers from public data. *Proceedings of the National Academy of Sciences of the United States of America (PNAS)*.

Adida, B., Bond, M., Clulow, J., Lin, A., Murdoch, S., Anderson, R. & R. Rivest (n.d.). Phish and Chips (Traditional and New Recipes for Attacking EMV). Available at: http://www.cl.cam.ac.uk/~rja14/Papers/Phish-and-Chips.pdf (last accessed July 14, 2010): 1 – 2.

Adviescommissie Informatiestromen Veiligheid (2007). *Data voor daadkracht. Gegevensbestanden voor veiligheid: observaties en analyse*.

Anderson, R. (2001). Why Information Security is Hard - An Economic Perspective. *Proceedings of the 17th Annual Computer Security Applications Conference:* 358-366.

_____ & T. Moore (2006). The Economics of Information Security. *Science*, Vol. 314.

_____, Böhme, R., Clayton, R. & T. Moore (2008). *Security, Economics, and the Internal Market*. Report commissioned by the European Network and Information Security Agency (ENISA).

Australasian Centre for Policing Research (ACPR) (2006). *Review of the legal status and rights of victims of identity theft in Australasia.*

Australian Institute of Criminology (2007). Money Mules. *High Tech Crime Brief*.

Baer, M. H. (2008). Linkage and the Deterrence of Corporate Fraud. *Virginia Law Review*, Vol. 94.

Basel Committee on Banking Supervision (2001). *Customer due diligence for banks*.

Beck, U. (1992). *Risk Society: Towards a New Modernity*. London: SAGE.

Bellia, P. L. (2009). Federalization in Information Privacy Law. *Yale Law Journal*, Vol. 118: 868 – 900.

Bennett, C. J. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. New York: Cornell University Press.

_____ (2001). 'Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?' in P.E. Agre & M. Rotenberg (eds.). *Technology and Privacy: The New Landscape*. Cambridge, MA: MIT Press: 99 – 124.

Bennison, P. F. & J. P. Lasher (2004). 'Data Security Issues Relating to End of Life Equipment', *Proceedings of the 2004 IEEE International Symposium on Electronics and the Environment*.

Berghel, H. (2000). Identity Theft, Social Security Numbers, and the Web. *Communications of the ACM*, Vol. 43 (2).

Biegelman, M. T. (2009). *Identity Theft Handbook: Detection, Prevention, and Security*. Hoboken, NJ: John Wiley & Sons, Inc.

Bilge, L., Strufe, T. Balzarotti, D. & E. Kirda (2009). All Your Contacts Are

Belong to Us: Automated Identity Theft Attacks on Social Networks. Paper presented at the *18th International World Wide Web Conference*. Available at : http://www.csd.uoc.gr/~hy558/papers/p551.pdf (last accessed July 14, 2010) : 551 – 560.

Binder, R. & M. Gill (2005). *Identity Theft and Fraud: Learning From the USA*. Perpetuity Research & Consultancy International Ltd.

Bits of Freedom (BOF) (2010). *Position paper meldplicht datalekken*. Available at: https://www.bof.nl/live/wp-content/uploads/2010/01/datalekken-def.pdf (last accessed July 12, 2010).

Blok, P. (2002). *Het recht op privacy*; *Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*. Den Haag: Boom Juridische Uitgevers.

Boer, L. & T. K. Grimmius (2009). *Melding Maken? Internationale quick scan meldplicht gegevens verlies*. Study Commissioned by the Ministry of Economic Affairs.

Bowal, P. (1999). Reluctance to regulate: the case of negative option marketing. *American Business Law Journal*, Vol. 36 (2): 377 – 390.

Brady, R. (2007). *From Court to Country: A Legal, Social and Political Analysis of Privacy in the U.S., 1965-1974*. Available at: http://digitalcommons.macalester.edu/cgi/viewcontent.cgi?article=1004 &context=poli_honors (last accessed July 12, 2010).

Brand, M., Champion, A. & D. Chan (2007). Combating the Botnet Scourge. Available at : http://www.cse.ohiostate.edu/~champion/research/Combating_the_B otnet_Scourge.pdf (last accessed July 14, 2010).

Bratman, B. E. (2002). Brandeis and Warren's *The Right to Privacy* and the Birth of the Right to Privacy. *Tennessee Law Review*, Vol. 69: 623 – 652.

Breinholt, J. (2005). How about a little perspective: The USA Patriot Act and the uses and abuses of History. *Texas Review of Law & Politics*, Vol. 9: 17 – 62.

Brenner, S. W. & L. L. Clarke (2005). Distributed Security: A New Model of Law Enforcement. *SSRN Accepted Papers Series*.

Brenner, S. W. (2007). 'The Council of Europe's Convention on Cybercrime,' in J. M. Balkin, J. Grimmelmann, E. Katz, N. Kozlovski, S. Wagman & T. Zarsky (eds.) *Cybercrime: Digital Cops in a Networked Environment*. New York: New York University Press: 207 – 220.

Brooks, N. (2005). *Data Brokers: Background and Industry Overview*. Congressional Research Service (CRS) Report to Congress.

Brown, K., Mcllveen, H. & C. Strugnell (2000). Nutritional awareness and food preferences of young consumers. *Nutrition & Food Science*, Vol. 30 (5): 230-235.

Bruhn, C. M. (1997). Consumer Concerns: Motivating to Action. *Emerging Infectious Diseases*, Vol. 3 (4): 511 – 515.

Burge, W. L. (1973). Testimony to the U.S. Senate Subcommittee on Consumer Credit of the Committee on Banking, Housing and Urban Affairs. *Fair Credit Reporting Act—1973*, Hearing, October 1, 1973.

Burns, P. & A. Stanley (2002). *Fraud Management in the Credit Card Industry*. Discussion Paper Payment Cards Center, Federal Reserve Bank of Philadelphia.

Byrne, J. (1993). The Bank Secrecy Act: Do Reporting Requirements Really Assist the Government? *Alabama Law Review*, Vol. 44: 801 – 838.

Canadian Anti-Fraud Centre Criminal Intelligence Analytical Unit (2010). *Mass Marketing Fraud & ID Theft Activities*. Annual Statistical Report 2009.

Carafano, J. J. (2008). Making REAL ID Real—Finally. *WebMemo*, Heritage Foundation.

Carlson, E. L. (2006). Phishing for Elderly Victims: As the Elderly Migrate to the Internet Fraudulent Schemes Targeting Them Follow. *Elder Law Journal*, Vol. 14: 423 - 427.

Cate, F. H., Litan, R. E., Staten, M. & P. Wallison (2003). *Financial Privacy, Consumer Prosperity, and the Public Good: Maintaining the Balance*. Washington, DC: American Enterprise Institute Press.

Cate, F. H. (2004). Testimony to the U.S. House Subcommittee on Social Security of the Committee Ways and Means. *Enhancing Social Security Number Privacy*, Hearing, June 15, 2004 (Serial 108-59).

_____ (2008). Government Data Mining: The Need for a Legal Framework. *Harvard Civil Rights Civil Liberties Review*, Vol. 43.

Cavoukian, A. (1997). *Identity Theft: Who's Using Your Name?* Information and Privacy Commissioner/Ontario.

Centraal Meldpunt Identiteitsfraude (2010). *Jaarrapportage 2009*.

Chandler, J. A. (2006). Liability for Botnet Attacks. *Canadian Journal of Law and Technology*, Vol. 5 (1): 13 – 25.

Cheney, J. S. (2005). *Do Definitions Still Matter?* Discussion Paper Payment Cards Center, Federal Reserve Bank of Philadelphia.

_____ (2010). *Heartland Payment Systems: Lessons Learned from a Data Breach*. Discussion Paper Payment Cards Center, Federal Reserve Bank of Philadelphia.

Cheng, K. T. (2008). Identity Theft and the Case for a National Credit Report Freeze Law. *North Carolina Banking Institute*, Vol. 12.

Cicero, M. T. (44 B.C.). *De Legibus*. Book III.

Clarke, R. V. G. (1980). "Situational" Crime Prevention: Theory and Practice. *British Journal of Criminology*, Vol. 20 (2): 136 – 147.

_____ (1992). 'Introduction,' in R.V. Clarke (ed.) *Situational Crime Prevention: Successful Case Studies*. Albany, NY: Harrow and Heston Publishers: 3 – 36.

_____ (1995). 'Situational Crime Prevention,' in M. Tonry & D. P. Farrington (eds.) *Building a Safer Society: Strategic Approaches to Crime Prevention*. Chicago: University of Chicago Press: 91 – 150.

_____ (1997). 'Introduction,' in R.V. Clarke (ed.) *Situational Crime Prevention: Successful Case Studies*. Second edition. Albany, NY: Harrow and Heston Publishers: 1 – 43.

_____ & G. R. Newman (2006). *Outsmarting the Terrorists*. Praeger Security International.

Clayton, R. (2005). Insecure real-world authentication protocols (or why phishing is so profitable). *Proceedings of 13th International Workshop on Security Protocols*.

Cody, J. P. (1999). Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation? *Catholic University Law Review*, Vol. 48: 1183 – 1236.

Cohen, L. E. & M. Felson (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review*, Vol. 44 (4): 588-608.

College Bescherming Persoonsgegevens (2003). *Onrechtmatig, onbehoorlijk en onzorgvuldig. De verwerking van persoonsgegevens door een handelsinformatiebureau voor rapportage van verhaalsinformatie.*

_____ (2005a). Advies wetsvoorstel algemene bepalingen burgerservicenummer.

_____ (2005b). Advies Wet gebruik BSN in de zorg.

_____ (2010a). Wetgevingsadvies CBP inzake wijziging Telecommunicatiewet.

_____ (2010b). Wetgevingsadvies - Wet gebruik BSN in de financiële sector.
Commissie Brouwer-Korf (2009). *Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer.*
Commissie Koopmans (1976). *Eindrapport van de Staatscommissie Bescherming Persoonlijke Levenssfeer in verband met Persoonsregistraties.* 's-Gravenhage: Staatsuitgeverij.
Commissie Simons (1968). *Rapport inzake verstrekking van inlichtingen uit de bevolkingsregisters.* 's-Gravenhage: Staatsuitgeverij.
Commissie Modernisering GBA (2001). *GBA in de toekomst. Gemeentelijke Basis Administratie persoonsgegevens als spil voor toekomstige identiteits-infratructuur.*
Commissie Westerhout (1970). *Rapport inzake registratie van persoonsgegevens.* 's-Gravenhage: Staatsuitgeverij.
Commission on Crime Prevention and Criminal Justice (2009). Thematic discussion: Economic fraud and identity-related crime. Eightteenth session, Vienna, 14 april 2009.
Commission of the European Communities (1990). Commission communication on the protection of individuals in relation to the processing of personal data in the community and information security. Brussels September 13, 1990.
Consumer Federation of America (CFA) (2009). T*o Catch a Thief: Are Identity Theft Prevention Services Worth the Cost?*
Copes, H. & L. Vieraitis (2007). *Identity Theft: Assessing Offenders' Strategies and Perceptions of Risk. Research report submitted to the United States Department of Justice.* Available at: http://www.ncjrs.gov/pdffiles1/nij/grants/219122.pdf (last accessed July 4, 2010).
_____ (2009). Understanding Identity Theft: Offenders' Accounts of Their Lives and Crimes. *Criminal Justice Review*, Vol. 34: 329 – 349.
Correll, S-P. & L. Corrons (2009). *The Business of Rogueware: Analysis of the New Style of Online Fraud.* Panda Security.
Crenshaw, A. B. (1996). Identity Crisis: The Theft that's though to thwart. *Washington Post*, 25 August 1996: H01.
Cuganesan, S. & D. Lacey (2003). *Identity fraud in Australia: an evaluation of its nature, cost and extent.* Standards Australia International.
Dadisho, E. (2005). Identity Theft and the Police Response: The Problem. *The Police Chief*, Vol. 72 (1).
Dahl, J. Y. & A. R. Saetnan (2009). "It all happened so slowly"–On controlling function creep in forensic DNA databases. *International Journal of Law, Crime and Justice*, Vol. 37: 83 – 103.
Dang, H. (2008). The Origins of Social Engineering. *McAfee Security Journa*l: 4-8.
Dantu, R., Palla, S. & J. Cangussu (2008). Classification of Phishers. *Journal of Homeland Security and Emergency Management*, Vol. 5 (1): 1- 14.
David, F. M., Chan, E.M., Carlyle, J. C. & R. H. Campbell (2008). Cloaker: Hardware Supported Rootkit Concealment. *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA: 296 – 310.
Davis, R. M. (1973). Testimony to the U.S. Senate Subcommittee on Consumer Credit of the Committee on Banking, Housing and Urban Affairs. *Fair Credit Reporting Act—1973*, Hearing, October 1, 1973.
De Nederlandsche Bank (2003). *Jaarverslag 2002.*
_____ (2008). *Jaarverslag 2007.*
_____ (2009a). *Jaarverslag 2008.*

_____ (2009b) SEPA Migration Plan for the Netherlands. Status and Planning June 2009.

Department of Homeland Security (2003). *The National Strategy to Secure Cyberspace.*

_____ (2009). Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes. 6 Code of Federal Regulation Part 37.

Dhamija, R., Tygar, J. D. & M. Hearst (2006). Why Phishing Works. *Proceedings of the Conference on Human Factors in Computing Systems.*

Dinerstein, M. (2003). *IDs for Illegals: The 'Matricula Consular' Advances Mexico's Immigration Agenda.* Backgrounder, Center for Immigration Studies.

Dinjens, M. (2010). Banken: Aantal slachtoffers van bankfraude ligt veel hoger. *Metro*, June 24, 2010: 3.

Directoraat-Generaal Rechtspleging en Rechtshandhaving (2006). Identiteitsvaststelling in de strafrechtketen.

Director Instrumentation Procedures and Maintenance of Law and Order (2010). Letter to the Steering Committee of the Strengthening Identification in the Public Sector Program.

Dirro, T. & D. Kolberg (2008). Germany: Malware learns the language. *Sage*: 22 – 27.

Dixon, P. (2006). *Medical Identity Theft: The Information Crime That Can Kill You.* Available at: http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf (last accessed July 4, 2010).

Dong, X., Clark, J. A., & J. Jacob (2008). Modelling User-Phishing Interaction. *2008 Conference on Human System Interactions*: 627-632.

Dubbeling, E. (2008). Gebruik Burgerservicenummer een 'must' voor banken. *Bank Wereld*, Vol. 2008 (1).

Dunham, K. & J. Melnick (2008). *Malicious Bots: An Inside Look.* Auerbach Publications.

Durham, K. (2006). Money Mules: An Investigative View. *EDPACS*, Vol. 33 (8): 13 – 19.

Dutch eGovernment Knowledge Centre (2005). *E-government in the Netherlands: a brief history.* Available at: http://www.todigitalworld.org/dl.php?id=21 (last accessed July 5, 2010).

Dutton, W. Guerra, G. A., Zizzo, D. J. & M. Peltu (2005). The cyber trust tension in E-government: Balancing identity, privacy, security. *Information Polity*, Vol. 10: 13 -23.

Van Eeten, M. J. G. & J. M. Bauer (2008). *Economics of Malware: Security Decisions, Incentives and Externalities.* STI Working Paper 2008/1.

Van Eeten (2010). *Techniek van de onmacht.* Nederlandse School voor Openbaar Bestuur.

Egele, M., Wurzinger, P., Kruegel, C. & E. Kirda (2009a). 'Defending Browsers against Drive-by-Downloads: Mitigating Heap-spraying Code Injection Attacks,' in U. Flegel & D. Bruschi (eds.) *Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer: 1 – 19.

Egele, M., Kruegel, C. & E. Kirda (2009b). Mitigating Drive-by Download Attacks: Challenges and Open Problems. Unpublished manuscript. Available at: https://www.iseclab.org/papers/inetsec09.pdf (last accessed July 14, 2010).

Egelman, S. & L. F. Cranor (2006). The Real ID Act: Fixing Identity Documents with Duct Tape. *I/S: A Journal of Law and Policy for the Information Society*, Vol. 2 (1): 149 – 183.

Electronic Privacy Information Center (EPIC) (2008). REAL ID Implementation Review: Few Benefits, Staggering Costs.

Ericson, R. V. & K. D. Haggerty (1997). *Policing the risk society*. Toronto: University of Toronto Press.

Ernst & Young (2009). *Burgers en eOverheid: Wat verwacht de burger van de dienstverlening door de gemeente?*
Available at:
http://www.ey.com/Publication/vwLUAssets/EY_2009_Burgers_en_eOverheid/$FILE/Ernst%20&%20Young_2009_Burgers%20en%20eOverheid_B.pdf (last accessed July 13, 2010).

Etalle, S. (2008). *Nice to know*. Inaugural lecture Eindhoven University of Technology, October 3, 2008.

European Commission (2007a). Towards a general policy on the fight against cybercrime. Communication from the Commission to the European Parliament, the Council and the Committee of Regions of 22 May 2007.

_____ (2007b). Report on the outcome of the Review of the EU regulatory framework for electronic communications networks and services in accordance with Directive 2002/21/EC and Summary of the 2007 Reform Proposals.

_____ (2007c). Proposal for a council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes.

_____ (2009). Declaration on data breach notification. Annex to Directive 2009/136/EC.

European Data Protection Supervisor (2008). *Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector* (Directive on privacy and electronic communications).

Europol (2003). *2003 European Union Organised Crime Report.*

Federal Bureau of Investigations (2006). *Financial Crimes Report to the Public Fiscal Year 2006*.

Federal Deposit Insurance Corporation (FDIC) (2004). *Putting an end to account hijacking identity theft.*

Federal Financial Institutions Examination Council (FFIEC) (2001). *Authentication in an Electronic Banking Environment.*

_____ (2005). *Authentication in an Internet Banking Environment.*

_____ (2006). Frequently Asked Questions on FFIEC Guidance on *Authentication in an Internet Banking Environment.*

Federal Trade Commission (2003). REPORT: *Federal Trade Commission Overview of the Identity Theft Program*. Available at:
http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/ftc_overview_id_theft.pdf (last accessed July 4, 2010).

_____ (2004). Final Rule. Available at:
http://www.ftc.gov/os/2004/10/041029idtheftdefsfrn.pdf
(last accessed July 4, 2010).

_____ (2008). *Security in Numbers: SSNs and ID Theft.*

_____ (2010). *Consumer Sentinel Network Data Handbook for January – December 2009.*

_____ (n.d.). Fighting Fraud with the Red Flags Rule: a How- to Guide for Businesses. Available at http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf

Feldmann, E. (2006). DigiD krijgt betere beveiliging na kritiek. Available at: http://webwereld.nl/nieuws/40711/digid-krijgt-betere-beveiliging-na-kritiek.html (last accessed July 13, 2010).

Feldman, S. (1974). The Fair Credit Reporting Act—From the Regulators Vantage Point. *Santa Clara Lawyer*, Vol. 14: 459 – 490.

Fellowes (2006). Nederlanders achteloos met privé en bedrijfsinformatie. Onderzoek: werknemers brengen eigen organisaties in gevaar. *Press release*, April 10, 2006.

_____ (2009). Nederlander niet bewust van risico identiteitsfraude. *Press Release.*

Felson, M. & L. E. Cohen (1980). Human Ecology and Crime: A Routine Activity Approach. *Human Ecology*, Vol. 8 (4): 389 – 406.

Felson, M. (1986). 'Linking Criminal Choices, Routine Activities, Informal Control, and Criminal Outcomes,' in D. B. Cornish & R. V. Clarke (eds.) *The Reasoning Criminal: Rational Choice Perspectives on Offending*. New York: Springer-Verlag: 119 – 128.

_____ (2006). *Crime and Nature*. SAGE Publishing.

Fenwick, W., John, E. & J. Stimac (2009). The Necessity of Egovernment. *Santa* Clara Computer & High Tech Law Journal, Vol. 25: 427-465.

Financial Action Task Force (FATF) (1990). *The Forty Recommendations of the Financial Action Task Force onMoney Laundering.*

Finklea, K. M. (2010). *Identity Theft: Trends and Issues*. Congressional Research Service (CRS). Report to Congress.

Fraud Prevention Expert Group (FPEG) (2007). *Report on Identity Theft/Fraud.*

Fredrikson, M., Martignoni, L., Stinson, E. & S. J. J. Mitchell (2008). A layered architecture for detecting malicious behaviors. *11th International Symposium on Recent Advances in Intrusion Detection (RAID 2008).*

Frei, S., Duebendorfer, T., Ollman, G. & M. May (2009). Understanding the Web browser threat: Examination of vulnerable online Web browser populations and the "insecurity iceberg."

Frenzel, L. D. (1977). Fair Credit Reporting Act: The Case for Revision. *Loyola of Los Angeles Law Review*, Vol. 10: 409 – 439.

Froomkin, A. M. (2009a). Government Data Breaches. *Berkeley Technology Law Journal*, Vol. 24 (3): 1019 – 1060.

_____ (2009b). 'Identity Cards and Identity Romanticism,' in I. Kerr, V. Steeves & C. Lucock (eds.) *Lessons From the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*. New York: Oxford University Press: 245 – 263.

Furletti, M. (2004). *Prepaid Card Markets & Regulation*. Discussion Paper Payment Cards Center.

Garland, D. (2001). *The Culture of Control Crime and Social Order in Contemporary Society*. Oxford: Oxford University Press.

Garner, E. L. (2008). *Is Comprehensive Federal Data Security Legislation Necessary to Protect U.S. Businesses, Consumers and the Government from Identity Theft and Other Crimes?* Master Thesis Johns Hopkins University

Gartner (2003). Gartner Says Identity Theft is up Nearly Eighty Percent. Press Release, July 21, 2003.

_____ (2007). Gartner Says Number of Identity Theft Victims Has Increased More Than 50 Percent Since 2003. Press Release, March 6, 2007.

Gatzlaff, K.M. & K.A. McCullough (2010). The Effect of Data Breaches on Shareholder Wealth. *Risk Management and Insurance Review*, Vol. 13 (1): 61 – 83.

General Accounting Office (GAO) (1979). Statement of Richard L. Fogel before the Subcommittee on General Oversight and Renegotiation House Committee on Banking, Finance and Urban Affairs on the Use of Currency and Foreign Account Reports to Detect Narcotics Traffickers.

_____ (GAO) (1981). *Bank Secrecy Act Reporting Requirements Have Not Yet Met Expectations, Suggesting Need for Amendment*.

_____ (1986). *Bank Secrecy Act: Treasury Can Improve Implementation of the Act*.

_____ (1998). *Identity Fraud. Information on Prevalence, Cost, and Internet Impact is Limited*. Briefing Report to Congressional Requesters.

_____ (1999a). *Government and Commercial Use of the Number is Widespread*. GAO-HEHS-99-28.

_____ (1999b). *Enhancing Federal Oversight of Internet Banking Activities*.

_____ (2002). *Identity Theft: Prevalence and Cost appear to be Growing*. Report to Congressional Requesters, GAO-02-363.

_____ (2003). *Planned e-Authentication Gateway Faces Formidable Development Challenges*. Report to the Committee on Government Reform and the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House of Representatives.

Geltzer, J. N. (2003). The New Pirates of the Caribbean: How Data Havens Can Provide Safe Harbors on the Internet Beyond Governmental Reach. *Southwestern Journal of Law & Trade in Americas*, Vol. 10: 433 – 454.

Gellman, R. (2001). 'Does Privacy Law Work?' ' in P. E. Agre & M. Rotenberg (eds.) *Technology and Privacy: The New Landscape*. Cambridge, MA: MIT Press: 193 – 218.

_____ & P. Dixon (2009). *Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers*. Available at: http://www.worldprivacyforum.org/pdf/WPF_RedFlagReport_09242008fs.pdf (last accessed July 4, 2010).

Gemeente Amsterdam & Politie Amsterdam-Amstelland (2009). *Evaluatie pilot Vermissing Document*.

George, A. L. & A. Bennett (2005). *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press.

Georgia Tech Information Security Center (2009). Emerging Cyber Threats Report 2009. Available at http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf (last accessed July 13, 2010).

Gerards, J. L. & E. J. Snijders (1993). De toekomst van Tiel: Bureau Registratie? *Bank-en Effectenbedrijf*.

Gercke, M. (2007). *Project on Cybercrime: Internet-related identity theft*. Discussion paper Economic Crime Division Directorate General of Human Rights and Legal Affairs.

Gerring, J. (2001). *Social Science Methodology: A Criterial Framework*. Cambridge: Cambridge University Press.

Giffin, J. (2010). The Next Malware Battleground. *IEEE Security & Privacy*, Vol. 8 (3): 74 – 76.

Gold, S. (2009). A Newsworthy year. *Infosecurity*, Vol. 6: 24-28.

GOVCERT (2009). *Trendrapport 2009*.

Government Accountability Office (GAO) (2004a). *FBI Transformation: Data Inconclusive on Effects of Shift to Counterterrorism-Related Priorities on Traditional Crime Enforcement*, Report Number GAO-04-1036.

_____ (2004b). *Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information*. GAO-04-11.

_____ (2007a). *Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain*.

_____ (2007b). *Personal Information: Data Breaches are Frequent but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*.

Grijpink, J. H. A. M. & J. E. J. Prins (2003). 'New Rules for Anonymous Electronic Transactions? An Exploration of the Private Law Implications of Digital Anonymity,' in C. Nicoll, J. E. J. Prins, M. J. M. van Dellen (eds.) *Digital Anonymity and the Law. Tensions and Dimensions*. Den Haag: TMC Asser Press: 249-269.

Grijpink, J. H. A. M. (2006). Identiteitsfraude en overheid. *Justitiële Verkenningen*, Vol. 32 (7): 37 – 57.

Grimmelman, J. (2009). Saving Facebook. *Iowa Law Review*, Vol. 94: 1137-1206.

Grizzard, J. B., Sharma, V., Nunnery, C. & B. B. Kang (2007). Peer-to-Peer botnets: Overview and Case Study. *Usenix Hotbots 2007*.

Groebner, V. (2007). *Who Are You? Identification, Deception, and Surveillance in Early Modern Europe*. New York: Zone Books.

Gross, R. & A. Acquisti (2005). Information Revelation and Privacy in Online Social Networks. (The Facebook Case). *Pre-proceedings version ACM Workshop on Privacy in the Electronic Society (WPES)*.

Grossklags, J. & A. Acquisti (2007). When 25 cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information. *Workshop on the Economics of Information Security (WEIS)*.

Gusfield, J. R. (1981). *The Culture of Public Problems: Drinking-Driving and the Symbolic Order*. Chicago: University of Chicago Press.

Hafkamp, W. & R. Steenvoorden (2009). 'Experience From the Financial Sector with Consumer Data and ICT Security,' in Z. Lukszo, G. Deconinck & M. P. C. Weijnen (eds.) *Securing Electricity Supply in the Cyber Age*, Springer Netherlands: 159 – 169.

Hansell, S. (1996). Identity Crisis: When a Criminal's Got Your Number. *New York Times*, June 16, 1996: 1.

Harley, D. & A. Lee (2007). Phish Phodder: is User Education Helping or Hindering? *17th Virus Bulletin and Conference Proceedings*.

Harper, J. (2006) *Identity Crisis*. Washington, DC: CATO Institute.

Harris Interactive (2003). *Identity Theft New Survey & Trend Report*. Commissioned by Privacy & American Business.

Hartle, R. (1998). Testimony to the U.S. Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary. *The Identity Theft and Assumption Deterrence Act*, Hearing, May 20, 1998 (Serial 105 - 779).

Health, Education, and Welfare Advisory Committee (1973). *Records, Computer, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*.

Hegt, S. (2008). *Analysis of Current and Future Phishing Attacks on Internet Banking Services*. Master Thesis Technical University Eindhoven.

Henderson, S. E. (2006) Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search. *Catholic University Law Review*, Vol. 55: 373 – 438.

_____ (2007). Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too. *Pepperdine Law Review*, Vol. 34 (4): 975 – 1026.

Heng, S. (2004). E-Payments: Modern Complement to Traditional Payment Systems. Deutsche Bank Research, Economics Working Paper 44.

Herley, C. (2009). So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. *Proceedings of the 2009 workshop on New Security Paradigms Workshop*: 133-144.

Hernon, P. & R. Cullen (2006). 'E-government: Transforming Government,' in P. Hernon, R. Cullen & H. C. Relyea (eds.) *Comparative Perspectives on E-government*: *Serving today and Building for Tomorrow*. Lanham, MD: Scarecrow Press: 3 – 21.

Het Expertise Centrum (HEC) (2007). Papernote 21: *Naar een goed gebruik van het burgerservicenummer*.

Hill, M. (2009). *The Public Policy Process*. Pearson Education Limited.

Hirschi, T. (1969). *Causes of Delinquency*. Berkeley: University of California Press.

Hoar, S. B. (2001). Identity Theft: The Crime of the New Millennium. *Oregon Law Review*, Vol. 80: 1423 – 1447.

Holden, S. H. & L. I. Millett (2005). Authentication, Privacy, and the Federal E-Government. *The Information Society*, Vol. 21 (5): 367 – 377.

Holz, T., Engelberth, M. & F. Freiling (2008). Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones. Available at: https://www.fehcom.net/fh-frankfurt/vorlesungen/2008_WS/itsec/material/impersonation-attacks-TR.pdf (last accessed July 14, 2010).

Home Office Statistical Bulletin (2007). *Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey*. Available at http://www.homeoffice.gov.uk/rds/pdfs07/hosb1007.pdf (last accessed July 12, 2010).

Hoofnagle, C. J. (2004). Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement. *North Carolina Journal of International Law and Commercial Regulation*.

_____ (2005). 'Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors,' in A. Chander, L. Gelman, M.J. Radin (eds.) *Securing Privacy in the Internet Age*. Stanford, CA: Stanford University Press.

_____ (2007). Identity Theft: Making the Known Unknowns Known. *Harvard Journal of Law and Technology*, Vol. 21 (1): 98 -122.

_____ (2009). Internalizing Identity Theft. *UCLA Journal of Law & Technology*, Vol. 13 (2): 1 – 36.

House of Lords: Science and Technology Committee (2007) Personal internet security: 5th report of session, Vol. 1: Report.

Hovey, M. T. (2009). Comment: Oh, I'm sorry, did that identity belong to you? How ignorance, ambiguity, and identity theft create opportunity for immigration reform in the United States. *Villanova Law Review*, Vol. 54.

Howard, H. M. (2005). The Negligent Enablement of Imposter Fraud: A Common Sense Law Claim. *Duke Law Journal*, Vol. 54: 1263-1294.

Huang, Y., Xianjun, G., & Whinston, A. (2007). Defeating DDoS attacks by fixing the incentive chain. *ACM Transactions on Internet Technology*, Vol. 7 (1).

Hughes, S. J. (1992). Policing Money Laundering Through Funds Transfers: A Critique of Regulation Under the Bank Secrecy Act. *Indiana Law Journal*, Vol. 67: 283 – 330.

Hunter, P. (2008). PayPal, FBI and others wage war on Botnet armies. Can they succeed? *Computer Fraud & Security*, Vol. 2008: 13 – 15.

Ianelli, N. & A. Hackworth (2007). Botnets as a Verhicle for Online Crime. *The International Journal of Forensic Computer Science*: 19 – 39.

Identity Theft Prevention and Identity Management Standards Panel (IDSP). (2009). *Workshop Report Identity Verification.*

Identity Theft Resource Center (2004). *Identity Theft: The Aftermath 2003.*

_____ (2005). *Identity Theft: The Aftermath 2004.*

_____ (2009). *Identity Theft: The Aftermath 2008.*

_____ (2010a). *Identity Theft: The Aftermath 2009.*

_____ (2010b). *2009 Data Breach Stats.*

_____ (2007). *Combating Identity Theft: A Strategic Plan.*

_____ (2008). *The President's Identity Theft Task Force Report.*

International Civil Aviation Organization (ICAO). (2003). Biometric Identification to Provide Enhanced Security and Speedier Border Clearance for the Travelling Public. *Press Release.*

Jakobsson, M. (2007). The Human Factor in Phishing. *Privacy & Security of Consumer Information* : 1 – 19.

Jamieson, R., Sarre, R., Steel, A. & G. Stephens (2008). Defining Identity Crimes. Paper presented at the 19th Australasian Conference on Information Systems, 3-5 December 2008 Christchurch.
Available at http://www.bsec.canterbury.ac.nz/acis2008/Papers/acis-0183-2008.pdf (last accessed July 4, 2010).

Javelin Strategy & Research (2005a). *2005 Identity Fraud Survey Report.* Consumer Version.

_____ (2005b). Phishing: Consumer Behavior and Awareness. Syndicated Report Brochure.

_____ (2006). *2006 Identity Fraud Survey Report.* Consumer Version.

_____ (2007a). *2007 Identity Fraud Survey Report.* Consumer Version.

_____ (2007b). New Report Shows Top U.S. Banks Succeeding in Identity Fraud Resolution, Slower Progress in Detection and Prevention Capabilities. *Press Release.*

_____ (2008). Consumer survey on data breach notification. Available at: http://www.tawpi.org/uploadDocs/Data_Breach_survey.pdf (last accessed July 12, 2010).

_____ (2009). *2009 Identity Fraud Survey Report: Consumer Version.*

_____ (2010). *2010 Identity Fraud Survey Report: Consumer Version.*

Jones, H. & J. H. Soltren (2005). *Facebook: Threats to Privacy.* Unpublished manuscript. Available at: http://groups.csail.mit.edu/mac/classes/6.805/student- papers/fall05-papers/facebook.pdf (last accessed July 13, 2010).

Johnson, I. D. (2010). Preventing Identity Theft and Other Financial Abuses Perpetrated Against Vulnerable Members of Society: Keeping the Horse in the Barn Rather than Litigating over the Cause and/or Consequences of His Leaving. *Pace Law Faculty Publications.*

Kabel, J. J. C. (2002). Centrale Kredietinformatie en verwerking van persoonsgegevens (I). *Privacy & Informatie*, nr. 6.
_____ (2003). Centrale Kredietinformatie en verwerking van persoonsgegevens (II). *Privacy & Informatie*, nr. 1.
Kaspersen, R. (2007). 'Het Cybercrime-verdrag van de Raad van Europa,' in E. J. Koops (ed.) *Strafrecht & ICT*. Den Haag: SDU Uitgevers: 137- 180.
Katel, P. (2005). Identity Theft: Can Congress Give Americans Better Protection? *The CQ Researcher*, Vol. 15 (22): 517-540.
Kennedy, T. R. (1969). The Plastic Jungle. *Montana Law Review*, Vol. 31: 29 – 50.
Kent, S. T. & L. I. Millett (2003). *Who Goes There? Authentication through the Lens of Privacy*. The National Academy of Sciences.
Kephart, J. (2010). *Fixing Flores: Assuring Adequate Penalties for Identity Theft and Fraud*. Backgrounder, Center for Immigation Studies.
Kerr, O. S. (2009). The Case for the Third-Party Doctrine. *Michigan Law Review*, Vol. 107: 561 – 602.
King, G. S. (1991). Statement to the U.S. House Subcommittee on Social Security of the Committee on Ways and Means. *Use of Social Security Number as a National Identifier*. Hearing, February 27, 1991 (Serial 102 -11).
Kingdon, J. W. (2003). *Agendas, alternatives, and public policies*. Longman, New York.
Kini, S. M. & J. T. Shreve (2006). Notice Requirements: Common Themes and Differences in the Regulatory and Legislative Responses to Data Security Breaches. *North Carolina Banking Institute*, Vol. 10: 87 – 108.
Knopjes, F. & J. Loogman (2008). *Quick scan werking identiteitsinfrastructuur*. Programma Identiteitsmanagement.
Kolodinsky, J. M., Hogarth, J. M. & M. A. Hilgert (2004). The adoption of electronic banking technologies by US consumers. *The International Journal of Bank Marketing*, Vol. 22 (4): 238-259.
Koninklijke Marechaussee (2003). *Rapport identiteitsfraude en (reis)documenten*.
Koops, B. J. (2001). Een nieuwe GBA, digitale kluisjes en identificatiedrang. *Nederlands Juristenblad*, Vol. 32: 1555-1561.
Koops, E. J. & R. E. Leenes (2006). 'ID Theft, ID Fraud and/or ID-related Crime. Definitions matter.' *Datenschutz und Datensicherheit*, Vol. 30 (9): 553-556.
_____, Leenes, R. E., Meints, M., Meulen, N. S. van der, & Jaquet-Chiffelle, D. O. (2009). A typology of identity-related crime: Conceptual, technical, and legal issues. *Information, communication & society*, Vol. 13 (1): 1-24.
Korps Landelijke Politiediensten (KLPD) (2007). Prioriteiten KLPD 2008-2011.
_____ (2008). Georganiseerde bovenregionale vermogenscriminaliteit. Verslag van een onderzoek voor het Nationaal dreigingsbeeld 2008.
Kosse, A. (2009). Creditcargebruik in Nederland: Een onderzoek naar de beleving en het gedrag van Nederlandse Consumenten. *De Nederlandsche Bank*.
KPMG (2006). *Ontvangen signalen voor een efficiënte identificatie*. Report to the Ministry of Finances.
Krebs, B. (2005). Computers seized in data-theft probe. *Washington Post*. May 19, 2005. Available at: http://www.washingtonpost.com/wp-dyn/content/article/2005/05/19/AR2005051900704.html (last accessed July 5, 2010).
_____ (2007). Is Cyber Crime Really the FBI's No. 3 Priority? Available at: http://voices.washingtonpost.com/securityfix/2007/09/is_cyber_crime_a_distant_3rd_p.html (last accessed July 4, 2010).

_____ (2008). 'Money Mules' Help Haul Cyber Criminals' Loot. *Washington Post*. January 25, 2008. Available at: http://www.washingtonpost.com/wp-dyn/content/story/2008/01/25/ST2008012501460.html (last accessed July 13, 2010).

_____ (2009). Payment Processor Breach May Be Largest Ever. *Washington Post*. Available at: http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html (last accessed July 5, 2010).

_____ (2010). FBI Promises Action Against Money Mules. Available at: http://krebsonsecurity.com/2010/05/fbi-promises-action-against-money-mules/ (last accessed July 13, 2010).

Kuitenbrouwer, F. (1991). *Het recht om met rust gelaten te worden*. Amsterdam: Uitgeverij Balans.

Kunst, M. J. J. & J. van Dijk (2009). *Slachtofferschap van Fraude: Een explorerend onderzoek naar de impact van diverse vormen van financieel-economische criminaliteit*.

Kyl, J. (1998). Opening statement to the U.S. Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary. *The Identity Theft and Assumption Deterrence Act*, Hearing, May 20, 1998 (Serial 105 – 779): 1.

Lane, G. W. (2008). *Geographies of Identity Theft in the U.S.: Understanding Spatial and Demographic Patterns, 2002-2006*. Master of Science Thesis Texas A&M University.

Lambrinoudakis, C., Gritzalis, S., Dridi, F. & G. Pernul (2003). Security requirements for e- government services: a methodological approach for developing a common PKI-based security policy. *Computer Communications*, Vol. 26 (16): 1873 – 1883.

Lauer, J. (2008). *The Good Consumer: Credit Reporting and the Invention of Financial Identity in the United States, 1840-1940*. Dissertation, University of Pennsylvania.

Laylock, G. (2004). New Challenges for Law Enforcement. *European Journal on Criminal Policy and Research*, Vol. 10: 39 – 53.

Le Comte, M. (2009). Een groeiende golf van credit card frauds. Een kwestie van pompen, verzuipen of een dam bouwen? *Bank- en Effectenbedrijf*, July/August 2009: 14 – 18.

Le Lievre, E. & R. Jamieson (2005). *An Investigation of Identity Fraud in Australian Organisations*. Collaborative Electronic Commerce Technology and Research (CollECTeR): 1-10.

Lenard, T. M. & P. H. Rubin (2006). Much Ado About Notification. *Regulation*, Vol. 29 (1): 44-50.

_____ (2009). In Defense of Data: Information and the Costs of Privacy. *Technology Policy Institute Working Paper*.

LexisNexis (2005). LexisNexis Concludes Review of Data Search Activity, Identifying Additional Instances of Illegal Data Access. *Press Release*. Available at: http://www.lexisnexis.com/about/releases/0789.asp (last accessed on July 5, 2010).

Lichtman, D.& E. Posner (2004). *Holding Internet Service Providers Accountable*. University of Chicago Law & Economics Working Paper.

Lilly, J. R. (2003). National Security at what price? A look into civil liberties concerns in the information age under the USA Patriot Act of 2001 and a proposed constitutional test for future legislation. *Cornell Journal of Law & Public Policy*, Vol. 12: 447 – 472.

Linnhoff, S. & J. Langenderfer (2004). Identity Theft Legislation: The Fair and Accurate Credit Transactions Act of 2003 and the Road Not Taken. *Journal of Consumer Affairs*, Vol. 38 (2): 204-216

Lodder, A. (2007). *eID Interoperability for PEGS. National profile of the Netherlands.* iDABC European E-government Services.

Locke, J. (1690). *Second Treatise on Government.*

Lombardi, R. (2006). Myths about identity theft debunked by experts. Available at http://www.itworldcanada.com/news/myths-about- identity-theft-debunked-by-experts/98501 (last accessed July 14, 2010).

LoPucki, L. M. (2001). Human Identification Theory and the Identity Theft Problem. *Texas Law Review*, Vol. 80: 89 – 134

Ludington, S. (2006). Reigning in the Data Traders: A Tort for the Misuse of Personal Information. *Maryland Law Review*, Vol. 66: 140 – 193.

Lütter, G. & R. van Troost (2006). *De Dataloods and zijn machinekamer; Inleiding tot de GBA.* Alphen aan de Rijn: Kluwer.

Lynch, J. (2005). Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks. *Berkeley Technology Law Journal*, Vol. 20: 259 – 300.

Maatschappelijk Overleg Betalingsverkeer (2006). *Rapportage Maatschappelijk Overleg Betalingsverkeer 2005*.

_____ (2008). *Rapportage Maatschappelijk Overleg Betalingsverkeer 2007*.

_____ (2009). *Rapportage Maatschappelijk Overleg Betalingsverkeer 2008*.

Majone, G. (1989). *Evidence, Argument, & Persuasion in the Policy Process*. New Haven, CT: Yale University Press.

Malcolm (2003). Remarks before the OECD-APEC Global Forum. Available at: http://www.justice.gov/criminal/cybercrime/JGM_OECD.htm

Mandell, L. (1990). *The Credit Card Industry: A History*. Boston: Twayne Publishers.

Marron, D. (2008). "Alter Reality" Governing the Risk of Identity Theft. *British Journal of Crime and Criminology*, Vol. 48 (1): 20 - 38.

Martin, T. (2009). Phishing for Answers: Factors Influencing a Participant's Ability to Categorize Email. Unpublished manuscript. Available at: http://projects.csail.mit.edu/spamconf/SC2009/Tim_Martin/Martin_Phishingv2.doc (last accessed July 13, 2010).

Masse, T. & W. Krouse (2003). *The FBI: Past, Present, and Future*. Congressional Research Service (CRS). Report for Congress.

Matejkovic, J. E. & K. E. Lahey (2001). Identity Theft: no help for consumers. *Financial Services Review*, Vol. 10: 210 – 235.

McKelvey, B. (2001). Financial Institutions' Duty of Confidentiality to Keep Customer's Personal Information Secure from the Threat of Identity Theft. *University of California Davis Law Review*, Vol. 34: 1077 – 1128.

McLaughlin,L. (2004). Bot Software Spreads, Causes New Worries. *IEEE Distributed Systems Online*, Vol. 5 (6): 1 – 5.

McMahon, R. B. (2004). After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why is Identity Theft the Most Prevalent Crime in America? *Villanova Law Review*, Vol. 49: 625 – 660.

McNally, M. M. (2008). *Trial by Circumstance: Is Identity Theft a Modern-Day Moral Panic?* Dissertation Graduate School Newark Rutgers, the State University of New Jersey.

McNamara, R. M. (1973). The Fair Credit Reporting Act: A Legislative Overview. *Journal of Public Law*, Vol. 22: 67 – 101.

McPherson, D. (2010). Cybercrime - A game of cat and mouse in 2009. *Network Security*, Vol. 2010 (2): 15 – 18.

Van der Meulen, N. S. (2007). The Spread of Identity Theft: Developments and Initiatives within the European Union. *The Police Chief*, Vol. 74 (5): 59-61.

_____ & E. J. Koops, eds. (2008). *D 12.7: Identity-related crime in Europe – Big Problem or Big Hype?* Available at: http://www.fidis.net.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2003). *Onderzoek naar de toepassing van biometrische kenmerken in de Nederlandse reisdocumenten*. Den Haag, Project Biometrie Agentschap BPR.

_____ (2005). *2b or not to 2b.* Evaluatierapport biometrieproef 2b or not 2b.

_____ (2007). *Auditrapport. Audit Modernisering GBA.*

Ministerie van Justitie (2007). Kabinet: 'bestrijding georganiseerde misdaad versterken.' *Press Release*. December 13, 2007.

_____ (2010). *Verantwoording veiligheid begint bij voorkomen.*

Mitchison, N., Wilikens, M., Breitenbach, L., Urry, R. & S. Portesi (2004). *Identity Theft: A Discussion Paper*. European Commission Joint Research Center.

Mitnick, K., Simon, W. & S. Wozniak (2002). *The art of deception: controlling the human element of security*. John Wiley & Sons.

Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General (2008). *Final Report Identity Crime*.

Mooij, J. & T. Dongelmans (2004). *Mogen wij even afrekenen? Twee eeuwen betalen in Nederland*. Amsterdam: Boom.

Moore, T. & R. Clayton (2008). The Impact of Incentives on Notice and Take-down. *Workshop on the Economics of Information Security (WEIS)*.

Moore, T., Clayton, R. & R. Anderson (2009). The Economics of Online Crime. *Journal of Economic Perspectives*, Vol. 23 (3).

Moynihan, D. & A. Roberts (2002). 'Public Service Reform and the New Security Agenda,' in *Governance & Public Security*. Washington, DC: Campbell Public Affairs Institute: 129-146.

Mul, V. (1999). *Banken en witwassen*. Sanders Instituut: Gouda Quint.

Muller, E. R., Kummeling, H. R. B. M. & R. P. Bron (2007). *Veiligheid en privacy: Een zoektocht naar een nieuwe balans*, Den Haag.

Nadelmann, E. A. (1986). Unlaundering Dirty Money Abroad: U.S. Foreign Policy and Financial Secrecy Jurisdictions. *Inter-American Law Review*, Vol. 18: 33 – 82.

National Commission on Terrorist Attacks upon the United States (2004). *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States.*

National Governors Association (2006). The Real ID Act: National Impact Analysis. Available at: http://www.nga.org/Files/pdf/0609REALiD.pdf (last accessed July 13, 2010).

De Nationale Ombudsman (2009). *De burger in de ketens*. Verslag van de Nationale ombudsman over 2008.

Nederlandse Vereniging van Banken (NVB). (2005). *Position paper: Banken en Burgerservicenummer (BSN).* Available at:

http://www.nvb.nl/scrivo/asset.php?id=18191 (last accessed July 12, 2010).

Newman, G. R. & R. V. Clarke (2003). *Superhighway Robbery: Preventing e-commerce crime*. Willian Publishing.

Newman, G. R. & M. M. McNally (2005). *Identity Theft Literature Review*. Research report submitted to the United States Department of Justice. Available at: http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf (last accessed July 4, 2010).

Newman, G. R. (2009). Policy Thoughts on "Bounded rationality of identity thieves." *Criminology & Public Policy*, Vol. 8 (2): 271 – 278.

Nixon, R. (1974). Radio Address about the American Right of Privacy. Available at: http://www.presidency.ucsb.edu/ws/index.php?pid=4364 (last accessed July 12, 2010).

Noiriel, G. (1996). *The French Melting Pot: Immigration, Citizenship, and National Identity*. Translated by Geoffrey de Laforcade. Minneapolis: University of Minnesota Press.

Office of the Inspector General. (2004). *The Internal Effects of the Federal Bureau of Investigation's Reprioritization*. Audit Report 04-39.

_____ (2005). *The External Effects of the Federal Bureau of Investigation's Reprioritization Efforts*. Audit report 05-37.

_____ (2010). *The Department of Justice's Efforts to Combat Identity Theft*. Audit Report 10-21.

Office of Management and Budget (2000). Implementation of the Government Paperwork Elimination Act. Available at: http://www.whitehouse.gov/omb/fedreg_gpea2/ (last accessed July 5, 2010).

O'Harrow, R. (1998). Who's Got Your Number? Data Access Feeds a New Breed of Crime. *Washington Post*, March 10, 1998: A08.

_____ (2005). ID Data Conned From Firm. *Washington Post*, February 17, 2005: E01.

_____ (2006). *No Place to Hide*. New York, NY: Free Press.

Oldenburg, D. (1997). Identity Theft and Other Scams. *Washington Post*, November 3, 1997: D05.

Olegario, R. (2001). Credit-Reporting Agencies: Their Historical Roots, Current Status, and Role in Market Development. Paper presented at the World Bank workshop *The Role of Credit Reporting Systems in the International Economy*, Washington DC. Available at: http://siteresources.worldbank.org/INTWDRS/Resources/477365-1257315064764/2429_olegario.pdf (last accessed July 5, 2010).

Ollmann, G. (2008). The evolution of commercial malware development kits and colour-by-numbers custom malware. *Computer Fraud & Security*, Vol. 28: 4 - 7.

Openbaar Ministerie (2006). *Perspectief op 2010*.

Organisation of Economic Co-Operation and Development (OECD) (2009). *Online Identity Theft*, OECD Publishing.

_____ (n.d.). Report on Identity Fraud: Tax Evasion and Money Laundering Vulnerabilities. Centre for Tax Policy and Administration.

Osborne, D. & T. Gaebler (1992). *Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector*. Reading, MA: Addison-Wesley Publishing Company, Inc.

O'Sullivan, O. (2004). ID Theft Overstated? Some Think So? *ABA Banking Journal*, Vol. 96: 8 – 9.

Overkleeft-Verburg, G. (1995). *De wet persoonsregistraties: norm, toepassing en evaluatie*. Zwolle: Tjeenk Willink.

Oxley, M. G. (2005). Opening statement to the U.S. House Committee on Financial Services (2005). *Assessing data security: preventing breaches and protecting sensitive information*, Hearing, May 4, 2005 (Serial 109 – 23): 2.

Panko, R. (2004). Banking on the USA Patriot Act: An Endorsement of the Act's Use of Banks to Combat Terrorist Financing and a Response to its Critics. *SSRN Working Paper Series*.

Pastrikos, C. (2004). Identity Theft Statutes: Which will protect Americans the most? *Albany Law Review*, Vol. 67: 1137 – 1157.

Pennathur, A. K. (2001). "Clicks and bricks": e-Risk Management for banks in the age of the Internet. *Journal of Banking & Finance*, Vol. 25: 2103 – 2123.

Perl, M. W. (2003). It's Not Always about the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft. *Journal of Criminal Law & Criminology*, Vol. 94: 169 – 208.

Perrin, S. (2006). *PIPEDA and Identity Theft: Solutions for Protecting Canadians*. BC Freedom of Information and Privacy Association.

Perry, J. M. (2005). Statement to the U.S. House Subcommittee on Oversight and Investigations of the Committee on Financial Services. *Credit Card Data Processing: How Secure is it?* Hearing, July 21, 2005 (Serial 109 – 48).

Plotkin, M. E. & B. J. Sanford (2006). Patriot Act: The Customer's View of "Know Your Customer"–Section 326 of the USA Patriot Act. *Bloomburg Corporate Law Journal*, Vol. 1.

Pontell, H. N. & G. Geis (2007). 'New Times, New Crimes: "Blocking" Financial Identity Fraud,' in F. Bovenkerk & M. Levi (eds.) *The Organized Crime Community*: *Essays in Honor of Alan A. Block*. New York: Springer.

_____, Brown, G. C. & A. Tosouni (2008). "Stolen Identities: A Victim Survey," in M. M. McNally & G. R. Newman (eds.) *Perspectives on Identity Theft. Crime Prevention Studies*. Monsey, NY: Criminal Justice Press.

Potter, B. (2008). How bad is it? *Network Security*, Vol. 2008: 18-20.

Pounder, C. (2008). Nine Principles for Assessing Whether Privacy is Protected in a Surveillance Society. *Identity in the Information Society*, Vol. 1 (1).

Prins, J. E. J., van de Donk, W. B. H. J., van Duiveboden, H. P. M., ten Have, K., Nouwt, J., Vorselaars, H. A. C. M. & S. Zouridis (1995). *In het licht van de Wet Persoonsregistraties: zon, maan of ster?* Alphen aan de Rijn: Samson Bedrijfsinformatie bv.

Prins, J. E. J. (2003). Het BurgerServiceNummer en de strijd tegen Identiteitsfraude. *Computerrecht* (1): 2-3.

_____ (2006). Variaties op een thema: van paspoort- naar identiteitsfraude. *Nederlands Juristenblad,* Vol. 81: 9-14.

_____ (2006). 'Property and Privacy: European Perspectives and the Commodification of Our Identity,' in L. Guibault & P.B. Hugenholtz (eds.), *The Future of the Public Domain*, Kluwer Law International: 223 – 257.

_____ (2007). 'National perspectives on e-government and required regulatory change', in J. E. J. Prins (ed.) *Designing E-Government*.

_____ & J. M. A. Berkvens (2007). 'De Wet Bescherming Persoonsgegevens,' in J. E. J. Prins & J. M. A. Berkvens (eds.) *Privacyregulering in theorie en praktijk*. Deventer: Kluwer*:* 25 – 46.

Privacy Rights Clearinghouse (2000). *Nowhere to Turn: Victims Speak Out on Identity Theft* - A Survey of Identity Theft Victims and Recommendations for Reform. Available at: http://www.privacyrights.org/ar/idtheft2000.htm (last accessed July 5, 2010).

_____ (2010). Chronology of Data Breaches Security Breaches 2005-Present. Available at: http://www.privacyrights.org/data-breach (last accessed July 5, 2010).

Provos, N., McNamee, D., Mavrommatis, P., Wang, K. & N. Modadugu (2008). The Ghost In The Browser Analysis of Web-Based Malware. Available at: http://www.usenix.org/event/hotbots07/tech/full_papers/provos/provos.pdf (last accessed July 13, 2010).

Proxmire, W. (1973) Opening statement to the U.S. Senate Subcommittee on Consumer Credit of the Committee on Banking, Housing and Urban Affairs. *Fair Credit Reporting Act—1973*, Hearing, October 1, 1973.

Rabobank Groep (2009). *Maatschappelijk jaarverslag 2008: Verantwoord bankieren voor een duurzame toekomst.*

Rackow, S. (2002). How the USA Patriot Act will permit governmental infringement upon the privacy of Americans in the name of "intelligence" investigations. *University of Pennsylvania Law Review*, Vol. 150: 1651 – 1696.

Ramasastry, A. (2004). 'Hooking Phishermen.' Available at: http://www.cnn.com/2004/LAW/08/16/ramasastry.phishing. (last accessed July 13, 2010).

Razvi, S. K. (2005). To What Extent Should State Legislatures Regulate Business Practices As a Means of Preventing Identity Theft? *Albany Law Journal of Science and Technology*, Vol. 15: 639-666.

RDW (2007). Jaarverslag 2006. Available at: http://www.rdw.nl/NR/rdonlyres/201237AF-3B3A-49AC-8ABC-E2C4F0C756ED/0/RDW_Jaarverslag_2006.pdf (last accessed July 13, 2010).

_____ (2009). Het rijbewijs als sleutel tot de overheid. Business case voor een chip op het rijbewijs. Versie 0.91. Unpublished document.

Rebovich, D. J. (2009). Examining Identity Theft: Empirical Explorations of the Offense and the Offender. *Victims & Offenders*, Vol. 4 (4): 357 — 364.

Regan, P. M. (1995). *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill, NC: University of North Carolina Press.

_____ (2004). Old issues, new context: Privacy, information collection, and homeland security. *Government Information Quarterly*, Vol. 21: 481–497.

Registratiekamer (2001). *Onrechtmatige handelwijze van een handelsinformatiebureau.*

Reidenberg, J. R. (1992). Privacy in the Information Economy: A Fortress or Frontier for Individual Rights? *Federal Communications Law Journal*, Vol. 44: 195 – 244.

_____ (2001). E-Commerce and Transatlantic Privacy. *Houston Law Review*, Vol. 38: 717 – 749.

Reijerman, D. (2010). Thuiswinkel.org wil dat meer webwinkels 3D Secure gaan gebruiken. Available at: http://tweakers.net/nieuws/67644/thuiswinkel-punt-org-wil-dat-meer-webwinkels-3d-secure-gaan-gebruiken.html (last accessed July 13, 2010).

Relyea, H. C. (2006). 'Access and Security,' in P. Hernon, R. Cullen & H. C. Relyea (eds.) *Comparative Perspectives on E-government*: *Serving today and Building for Tomorrow*. Lanham, MD: Scarecrow Press: 139 – 163.

Riley, M. (1998). Statement to the U.S. Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary. *The Identity Theft and Assumption Deterrence Act*, Hearing, May 20, 1998 (Serial 105 - 779).

Roberts, M. (2003). Big Brother Isn't Just Watching You, He's Also Wasting Your Tax Payer Dollars: An Analysis of the Anti-Money Laundering Provisions of the USA Patriot Act. *Rutgers Law Review*, Vol. 56: 573 – 602.

Rochefort, D. A. & R. W. Cobb (1994). 'Problem Definition: An Emerging Perspective,' in D. A. Rochefort & R. W. Cobb (eds.) *The Politics of Problem Definition: Shaping the Policy Agenda*. University Press of Kansas.

Rode, L. (2007). Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security. *Houston Law Review*, Vol. 43 (5): 1597.

Rogers, J. S. (2003). Forged Facsimile Signatures and Basic Principles of the Law of the Check Collection System. *Bepress Legal Series*, paper 24.

Romanosky, S., Telang, R. & A. Acquisti (2009). Do Data Security Breach Laws Reduce Identity Theft? *SSRN Working Paper Series*. Available at: http://www.ssrn.com.

Rotenberg, M. (1991). The Use of the Social Security Number as a National Identifier. *Computers & Society*, 21(2-4): 13 – 19.

Rule, J. B. (1974). *Private Lives and Public Surveillance: Social Control in the Computer Age*. New York: Schocken Books.

_____, McAdam, D., Stearns, L. & D. Uglow (1980). *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies*. New York: Elsevier.

Rush, H. Smith, C., Kraemer-Mbula, E. & P. Tang (2009). *Crime online: Cybercrime and illegal innovation*. Research report *NESTA*.

Sabol, M. A. (1999). The Identity Theft Assumption and Deterrence Act of 1998. Do individual victims finally get their day in court? *Loyola Consumer Law Review*, Vol. 11 (3): 165 – 173.

Salem, J. A. (2003). Public and private sector interests in e-government: a look at the DOE's Pubscience. *Government Information Quarterly*, Vol. 20 (1): 13 – 27.

Saunders, K. M. & B. Zucker (1999). Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act. *International Review of Law, Computers and Technology*, Vol. 13 (2): 183 – 192.

Schermer, B. W. & T. Wagemans (2009). *Onze digitale schaduw. Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat*.

Van Schijndel, P. (2008). *Identiteitsdiefstal*. Master Thesis Leiden University. Available at: http://media.leidenuniv.nl/legacy/scriptie_vanschijndel.pdf (last accessed July 12, 2010).

Schneier, B. (2005). Two-Factor Authentication: Too Little, Too Late. *Communications of the ACM*, Vol. 48 (4): 136.

Schreft, S. L. (2007). Risks of Identity Theft: Can the Market Protect the Payment System? *Economic Review*, Fourth Quarter.

Schwartz, P. (1992). Data Processing and Government Administration: The Failure of the American Legal Response to the Computer. *Hastings Law Journal*, Vol. 43: 1321 – 1389.

_____ & E. J. Janger (2007). Notification of Data Security Breaches. *Michigan Law Review*, Vol. 105: 913 – 984.

Schwartz, P. (2009). Privacy and Preemption. *Yale Law Journal*, Vol. 118: 902 – 947.

Seifert, J. W. (2006). 'E-government in the United States,' in P. Hernon, R. Cullen & H. C. Relyea (eds.) *Comparative Perspectives on E-government: Serving today and Building for Tomorrow*. Lanham, MD: Scarecrow Press: 25 – 54.

_____ (2008). *Reauthorization of the E-Government Act: A Brief Overview*. Congressional Research Service. Report for Congress.

Seltzer, M. D. (1999). The New Threats to Financial Privacy: Is there Liability for Financial Institutions and Their New Antagonists, the Information Brokers? *Boston Bar Journal*, Vol. 43: 8 – 23.

Sentrop, J. W. (1985). *Privacy-bescherming in Nederland*. Deventer: Van Loghum Slaterus.

Shadegg, J. B. (1999). Statement to the U.S. House Committee on Commerce & the House Subcommittees on Telecommunications, Trade and Consumer Protection, and on Finance. *Identity Theft: Is There Another You?* Joint Hearing, April 12, 1999 (Serial 106-16).

Shaffer, G. (1999). The Power of EU Collective Action: The Impact of EU Data Privacy Regulation on US Business Practice. *European Law Journal*, Vol. 5 (4).

Sharp, T., Sherver-Neiger, A., Fremouw, W., Kane, J. & S. Hutton (2004). Exploring the Psychological and Somatic Impact of Identity Theft. *Journal of Forensic Science*, Vol. 49 (1): 131 – 136.

Shostack, A. & P. Syverson (2004). 'What Price Privacy? (and why identity theft is about neither identity nor theft),' in L. Jean Camp and S. Lewis, (eds.) *Economics of Information Security*. Norwell: Kluwer Academic: 129 – 142

Sienkiewicz, S. & M. Bochicchio (2002). The Future of E-Commerce Payments. Available at: http://www.phil.frb.org/payment-cards-center/events/conferences/2002/FutureECommerce_062002.pdf (last accessed July 5, 2010).

Slobogin, C. (2005). Transaction Surveillance by the Government. *Mississippi Law Journal*, Vol. 75: 139 – 192.

Smith, D. (2001). Statement to the U.S. House Subcommittee on Commerce, Trade and Consumer Protection of the Committee on Energy and Commerce. *The EU Data Protection Directive: Implications for the U.S. Privacy Debate*, Hearing, March 8, 2001 (Serial 107 – 19).

Smith, R. E. (1993) *The Law of Privacy Explained*. Providence, RI: Privacy Journal.

_____ (2000). *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*. Providence, RI: Privacy Journal.

Smith, R. M. (1969). Unsolicited Credit Cards Bother Bankers, Too. *New York Times*, September 9, 1969.

Sobel, R. (2002). The Demeaning of Identity and Personhood in National Identification Systems. *Harvard Law & Technology Journal*, Vol. 15 (2): 319 – 387.

Sociaal Economische Raad (1990). *Invoering sofi-nummer*. Advies 90/06.

Solove, D. J. (2003) Identity Theft and the Architecture of Vulnerability. *Hastings Law Journal*, Vol. 54: 1227 – 1276.

_____ (2004). *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press.

_____ & C. J. Hoofnagle (2006). A Model Regime of Privacy Protection. *University of Illinois Law Review*, Vol. 2006 (2): 357 – 404.

Somogy, D. (2006). Information Brokers and Privacy. *I/S: A journal of Law and Policy*, Vol. 2 (3): 901 – 926.

Song, C., Zhuge, J., Han, X. & Z. Ye (2010). Preventing Drive-by Download via Inter-Module Communication Monitoring. *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*: 124 -134.

Sovern, J. (2003). The Jewel of Their Souls: Preventing Identity Theft Through Loss Allocation Rules. *University of Pittsburgh Law Review*, Vol. 64 (2): 343 – 406.

_____ (2004). Stopping Identity Theft. *Journal of Consumer Affairs*, Vol. 38 (2).

Spafford, J. L. (1973). Testimony to the U.S. Senate Subcommittee on Consumer Credit of the Committee on Banking, Housing and Urban Affairs. *Fair Credit Reporting Act—1973*, Hearing, October 1, 1973.

Sparks, S. A. (2000). The Direct Marketing Model and Virtual Identity: Why the United States Should Not Create Legislative Controls on the Use of Online Consumers Personal Data. *Dickinson Journal of International Law*, Vol. 18 (3): 517 – 552.

Sproule, S. & N. Archer (2006). *Defining Identity Theft – A Discussion Paper*. Prepared for the Ontario Research Network in Electronic Commerce (ORNEC) Identity Theft Research Program.

Steenkamp, R. (2004). *In goed vertrouwen. Onrechtmatige gegevensverstrekking aan een handelsinformatiebureau.* Inspectie Werk en Inkomen.

Stelter, B. (2009). Facebook's Users Ask Who Owns Information. *New York Times*, February 16, 2009.

Stessons, G. (2008). *Money Laundering: A New International Law Enforcement Model.* Cambridge: Cambridge University Press.

Stichting Waakzaamheid Persoonsregistratie (SWP) (1988). Bureau Krediet-Registratie: Drie Miljoen Kredietnemers. *Privacy en Registratie* (2).

Stone, D. A. (1989). Causal Stories and the Formation of Policy Agendas. *Political Science Quarterly*, Vol. 104 (2): 281 – 300.

Strader, T. J. & M. J. Shaw (1997). Characteristics of electronic markets. *Decision Support Systems*, Vol. 21.

Sullivan, B. (2005). Database giant gives access to fake firms: ChoicePoint warns more than 30,000 they may be at risk. Available at: http://www.msnbc.msn.com/id/6969799/ (last accessed July 13, 2010).

Sullivan, C. (2009). Is Identity Theft Really Theft? *International Review of Law, Computers, and Technology*, Vol. 23 (1 & 2): 77 – 87.

Sullivan, R. J. (2010). The Changing Nature of U.S. Card Payment Fraud: Issues for Industry and Public Policy. *Workshop for the Economics of Information Security (WEIS).*

Sylvester, E. L. (2004). Identity Theft: Are the Elderly Targeted? *Connecticut Public Interest Law Journal*, Vol. 3 (2): 313 – 341.

Synovate (2003). *Federal Trade Commission – Identity Theft Survey Report.*

Tafel van Thijn (2002). *Persoonsnummerbeleid in het kader van identiteitsmanagement.*

Den Tex, C. (2010). Speech presented on SuperTU/Esday, Eindhoven, February 11, 2010.

TILT (2007). *Het gebruik van het sofinummer door private en semi-publieke partijen: feitelijke trends in gebruik en normering.* Interne notitie ten behoeve van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Torpey, J. (2001). 'The Great War and the Birth of the Modern Passport System,' in J. Caplan & J. Torpey (eds.) *Documenting Individual Identity*. Princeton, NJ: Princeton University Press: 256 – 269.

Turner, M. (2006). Towards a Rational Personal Data Breach Notification Regime. *Information Policy Institute*.

Ullman, C. M. (1972). Liability of Credit Bureaus after the Fair Credit Reporting Act: The Need for Further Reform. *Villanova Law Review*, Vol. 17: 44 – 72.

United Kingdom Cabinet Office (2002). *Identity Fraud: A Study*. United Kingdom: Cabinet Office Publications.

United Nations (2005). Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Workshop 6: Measures to combat computer-related crime: Background paper.

United States Department of the Treasury (2005). *The Use of Technology to Combat Identity Theft*. Report on the Study Conducted Pursuant to Section 157 of the Fair and Accurate Credit Transactions Act of 2003.

United States Postal Investigation Services (2007). *Annual Report of Investigations of the United States Postal Services*.

United States Secret Service (2009). U.S. Secret Service Forms Three New Task Forces: Electronic crimes partnerships bring together law enforcement, academia and private sector. Press Release, July 10, 2009. Available at: http://www.secretservice.gov/press/GPA06-09_NewECTFs.pdf (last accessed July 4, 2010).

_____ (n.d.). *United States Secret Service Strategic Plan*. Available at: http://www.secretservice.gov/usss_strategic_plan_2008_2013.pdf (last accessed July 4, 2010).

UWV-GAK (2002). *Project Sofi-nummers 2000 – 2001. Onderzoek naar misbruik en oneigenlijk gebruik van Sofinummers.*

Vallance, C. (2008). Facebook faces privacy questions. Available at: http://news.bbc.co.uk/2/hi/technology/7196803.stm (last accessed July 13, 2010).

Valli, C. (2004). Throwing out the enterprise with the hard disk. *2nd Australian Computer, Networks & Information Forensics Conference*, School of Computer and Information Science, Edith Cowan University, Perth, Western Australia: 124-129.

Van Fleet, G. A. (1976). Judicial Construction of the Federal Credit Reporting Act: Scope and Civil Liability. *Columbia Law Review*, Vol. 76 (3): 458 – 507.

Vatsa, V., Sural, S. & A. K. Majumdar (2005). A Game-theoretic Approach to Credit Card Fraud Detection. *Proceedings of the International Conference on Information Systems Security*, Lecture Notes in Computer Science, Vol. 3803: 263 – 276.

Vedder, A., Van der Wees, L., Koops, E. J. & P. De Hert (2007). *Van privacyparadijs tot controlestaat*, Den Haag: Rathenau Instituut.

Vollaard, B. (2009). Does regulation of built-in security reduce crime? Evidence from a regression discontinuity approach. Paper presented at the first *Bonn/Paris Workshop on Law and Economics*, September 25-26.

De Vrede, T. (2010). Equens bestrijdt skimmen met computerkracht. *Automatiseringgids*.

De Vries, U. R. M. Th., Tigchelaar, H., van der Linden, M. & A. M. Hol (2007). *Identiteitsfraude: Een afbakening. Een internationale begripsvergelijking en analyse van*

nationale strafbepalingen. Den Haag: Wetenschappelijk Onderzoek en Documentatie Centrum (WODC).

Wales, E. (2003). E-commerce counts cost of Online Card Fraud. *Computer Fraud & Security*, Vol. 2003 (1): 9-11.

Warren, S. & L. D. Brandeis (1890). The Right to Privacy. *Harvard Law Review*, Vol. 4 (5): 193 – 220.

Weiss, J. A. (1989). The powers of problem definition: The case of government paperwork. *Policy Sciences*, Vol. 22: 97 – 121.

Weissink, A. M. J. (2010). Cyberbende koopt staatsloten. *Het Financiële Dagblad*. June 1, 2010.

Weistart, J. C. (1972). Consumer Protection in the Credit Card Industry: Federal Legislative Controls. *Michigan Law Review*, Vol. 70: 1475 – 1544.

Welfing, D. J. & P. J. M. Veugen (2008). *Identiteitscriminaliteit in een online omgeving*. TNO Rapport 34463. Draft version.

Werkgroep Betalingsverkeer Nederlandse Thuiswinkel Organisatie (2010). *Position Paper Online betalen in Nederland*.

Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum.

White, M. D. & C. Fisher (2008). Assessing Our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Efforts. *Criminal Justice Policy Review*, Vol. 19 (1): 3 – 24.

Whitley, E. A. & I. R. Hosein (2008). Departmental Influences on Policy Design. *Communications of the ACM*, Vol. 51 (5).

Whitson, J. R. & K. D. Haggerty (2008). Identity theft and the care of the virtual self. *Economy and Society*, Vol. 37 (4): 572 – 594.

Wijndelts, W. (2007). Overheid erkent fout met DigiD. *NRC Handelsblad*. Available at: http://www.nrc.nl/binnenland/article1785120.ece/Overheid_erkent_fout_met_DigiD (last accessed July 5, 2010).

Wildavsky, A. (1987). *Speaking Truth to Power: The Art and Craft of Policy Analysis*. London: Transaction Publishers.

Winer, J. M. (2001). Testimony to the U.S. House Subcommittee on Commerce, Trade and Consumer Protection of the Committee on Energy and Commerce. *The EU Data Protection Directive: Implications for the U.S. Privacy Debate*, Hearing, March 8, 2001 (Serial 107 – 19).

Winter, H. B., de Jong, P. O., Sibma, A., Visser, F. W., Herweijer, M., Klingenberg, A. M., & H. Prakken (2008). *Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet Bescherming persoonsgegevens in de praktijk*. Den Haag: Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC).

Withrow, C., Hand, D. J., Juszczak, P., Weston, D. & N. M. Adams (2009). Transaction Aggregation as a Strategy for credit card fraud detection. Data Mining and Knowledge Discovery, Vol. 18 (1): 30 – 55.

De Witt, R. (2006). Veel criminelen laten anderen straf uitzitten. *Elsevier*. Available at: http://www.elsevier.nl/web/Nieuws/Nederland/98552/Veel-criminelen-laten-anderen-straf-uitzitten.htm (last accessed July 12, 2010).

Wood, A. L. & O. F. Wahl (2006). Evaluating the Effectiveness of a Consumer-Provided Mental Health Recovery Education Presentation. *Psychiatric Rehabilitation Journal*, Vol. 30 (1): 46 – 53.

Woollacott, M. (1998). 'The Politics of Prevention,' in J. Franklin (ed.) *The Politics of Risk Society*. Cambridge: Polity Press: 120 – 123.

Wright, B. (2004). Internet Break-ins: New Legal Liability. *Computer Law & Security Report*, Vol. 20 (3): 171-174.

Zuckerberg, M. (2010). From Facebook, answering privacy concerns with new settings. *Washington Post*, May 24, 2010.

Zwenne, G. J., Duthler, A-W., Groothuis, M., Kielman, H., Koelewijn, W. & L. Mommers (2007). *Eerste fase evaluatie Wet bescherming persoonsgegevens Literatuuronderzoek en knelpuntenanalyse*. Den Haag: Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC).